

# **EXHIBIT A**

**IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA  
NORFOLK DIVISION**

DIRECTPACKET RESEARCH, INC.,

Plaintiff,

v.

POLYCOM, INC.,

Defendant.

Civil Action No. 2:18-cv-00331-AWA-RJK

**DEFENDANT POLYCOM, INC.’S OPENING CLAIM CONSTRUCTION BRIEF**

Pursuant to this court’s April 11, 2019 Agreed Order (D.I. 87), Defendant Polycom, Inc. (hereafter “Polycom”) hereby submits its opening claim construction brief for U.S. Patent Nos. 7,773,588 (“’588 Patent”), 7,710,978 (“’978 Patent”), and 8,560,828 (“’828 Patent”) (collectively, the “Asserted Patents”).

**I. LEGAL STANDARDS**

Claim construction begins with the words of the claim itself, which generally receive their ordinary and customary meaning as understood by a person of ordinary skill in the art at the time of the invention in the context of the specification and prosecution history. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312-13 (Fed. Cir. 2005) (*en banc*). Claim terms “can be defined only in a way that comports with the instrument as a whole[]” and must be read “in the context of the entire patent[.]” *Markman v. Westview Instruments, Inc.*, 517 U.S. 370, 389-90 (1996). A claim “is not entitled to a claim construction divorced from the context of the written description....” *Nystrom v. TREX Co.*, 424 F.3d 1136, 1144-45 (Fed. Cir. 2005) (*citing Phillips* 415 F.3d 1303.) In addition to the claims and specification, the Court may also consider the prosecution history of the patent and related patents. *Phillips*, 415 F.3d at 1317 (“Like the specification, the prosecution

history provides evidence of how the PTO and the inventor understood the patent.”); *Aventis Pharms. Inc. v. Amino Chems. Ltd.*, 715 F.3d 1363, 1375 (Fed. Cir. 2013) (citation omitted). Finally, it is also proper for the Court to consider extrinsic evidence such as inventor testimony, expert testimony, dictionaries, and treatises. *Phillips*, 415 F.3d at 1317-18.

## **II. BACKGROUND OF THE TECHNOLOGY**

The Asserted Patents purport to address certain aspects of communication between devices. The '978 and '828 Patents describe systems and methods for traversing a firewall. These patents describe that one way to ensure traffic makes it to its destination is to “tunnel” traffic through a so-called “commonly-open” port. The '588 Patent describes a system and method for communicating between incompatible protocols by converting each received packet in a first protocol, into an intermediate protocol; and then translating the intermediate protocol packets into a second protocol.

## **III. LEVEL OF ORDINARY SKILL IN THE ART**

A person of ordinary skill in the art would have had at least a Bachelor’s degree or equivalent in electrical engineering, computer engineering, or similar field, and at least two years’ experience in a relevant field such as designing communications networks. This experience could include, for example, experience in designing, implementing, monitoring and maintaining VoIP and multimedia networks. A person of ordinary skill in the art would therefore have at least some familiarity with the fundamentals of computer networks and related concepts, including VoIP, multimedia transmissions, protocol conversion, and well-known communication protocols such as SIP, H.323, and TCP/IP.

## **IV. CLAIM TERMS WITH AGREED UPON CONSTRUCTIONS**

### **A. U.S. Patent No. 7,773,588**

#### **1. protocol (claims 1, 3, 4, 6, 7, 8, 9, 11, 13, 14, 16, 17, 18, 20, 21, 23)**

The parties agree to the construction of “protocol,” as that term is used in the ’588 Patent, as “a set of conventions governing the format of messages exchanged between two communication devices.”

## V. CLAIM TERMS WITH DISPUTED CONSTRUCTIONS

### A. U.S. Patent No. 7,773,588

#### 1. first / second / [interim / intermediate] protocol (claims 1, 3, 4, 6, 7, 8, 9, 11, 13, 14, 16, 17, 18, 20, 21, 23)

| <i>Polycom’s Proposed Construction</i>  | <i>Plaintiff’s Proposed Construction</i>  |
|---|---|
| <p><u>Original Proposal:</u><br/>Each of the first, second and [interim / intermediate] protocols includes a signaling protocol, whereby no two signaling protocols are the same, and whereby a protocol is a set of rules or standards designed to enable computers to talk with each other.</p> <p><u>Compromise Proposed After Meet and Confer</u><br/>each of the first, second, and [interim / intermediate] protocols is different.</p> <p>a protocol is a set of conventions governing the format of messages exchanged between two communication devices, as set forth in the agreed-upon construction, <i>supra</i>.</p> | <p>No construction necessary.</p> <p>Alternatively:<br/>a [first / second / interim / intermediate] set of conventions governing the format of messages exchanged between two communication devices</p> |

Polycom’s original proposed construction of this claim term presented three issues for the Court to consider: (1) whether each of the first/second/[interim/intermediate] protocols are different from one another, (2) whether the protocols include a signaling protocol, and (3) the meaning of “protocol.” As set forth in § IV.A.1 *supra*, after meeting and conferring, and in an effort to narrow issues for the Court to consider, Polycom accepted directPacket’s construction of “protocol.” Thus, issue (3) no longer requires the Court’s attention. In light of the parties’ agreement on protocol, Polycom believes that issue (2), no longer requires the Court’s attention. While Polycom’s proposal that protocols include signaling protocols finds support in the



specification of the '588 patent (*see, e.g.*, '588 patent at 4:27-34 (discussing messaging and commands – *i.e.*, signaling)), and Polycom welcomes a construction including a requirement of a signaling protocol, Polycom believes the best use of the Court's resources is to decide the true dispute between the parties – whether the first, second, and [interim/intermediate] protocols have to be different from each other.<sup>1</sup> Polycom's position as seen in its original construction is that the protocols are required to be different. directPacket's construction, however, is silent as to whether the first, second, and [interim/intermediate] protocols are different. Because the intrinsic evidence confirms that they must be, and the patent specification clearly disclaimed systems in which the protocols are not different, the Court should reject directPacket's construction in favor of Polycom's originally proposed construction with the agreed definition of "protocol."

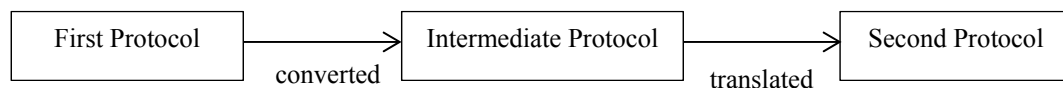
Claim construction begins with the claim language. Here the claims recite the words "first," "second," and "interim / intermediate" modifying the term "protocol," and those words must have some meaning and cannot be ignored. *See Ethicon Endo-Surgery, Inc. v. United States Surgical Corp.*, 93 F.3d 1572, 1582 (Fed. Cir. 1996), *citing Exxon Chemical Patents, Inc. v. Lubrizol Corp.*, 64 F.3d 1553, 1557 (Fed. Cir. 1995) (holding that all words in the claim must be given effect). The claim language requires "converting said first protocol into an intermediate protocol" and "translating said intermediate protocol into a second protocol" – confirming that

---

<sup>1</sup> While briefing this issue, it became apparent to Polycom that in light of the agreement on "protocol," it was no longer necessary to pursue a requirement that protocols contain signaling protocols, leaving only the dispute over whether the protocols need to be different. To further narrow the issues, on June 26, 2019, Polycom proposed a compromise construction directed to only that disputed issue for directPacket to consider. But, directPacket objects to Polycom offering a simplifying construction that focuses only where there is dispute, threatening to strike any such proposed construction. (*See Ex. 11.*) For completeness, Polycom identifies the narrowed construction on which it sought compromise with directPacket. *See Compromise Proposed After Meet and Confer* in table above.

the first, intermediate and second protocols are different. ('588 Patent at 7:31-35, 8:61-67, 9:58-10:7.) For example, if the first protocol is the H.323 protocol, then the second or intermediate protocol cannot also be the H.323 protocol.

The '588 Patent repeatedly purports to solve the problem of how to communicate between devices that utilize incompatible protocols - *i.e.*, different protocols. The '588 Patent purports to solve this problem by converting a first protocol into a second protocol via an intermediate protocol, whereby the intermediate protocol is “created to reflect the commonalities between the *various communication protocols* that are expected within the system.” ('588 Patent at 2:10-12.) In particular, the claims recite that the “first protocol” is “converted” into an “intermediate protocol” that is in turn “translated” into a “second protocol.” ('588 Patent at claims 1, 7, 11, 18.) The following illustrates the concept:



At the May 31, 2019 hearing, directPacket’s counsel explained that the '588 Patent is directed to communicating amongst systems that speak *different* languages. (D.I. 102 (May 31, 2019 Hearing Tr.) at 57:11-18.) Continuing this analogy, if the first and second languages are identical, there is no need to deploy the '588 Patent’s alleged invention. This logically makes sense because, if the first protocol is identical to the intermediate protocol, there is no reason to “convert;” and if the intermediate protocol is identical to the second protocol, there is no reason to “translate.”

The specification of the '588 Patent repeatedly makes clear that its purported invention is to solve the problem of communication between incompatible or *different* protocols, thereby disclaiming systems in which the protocols are not different. *See Luminara Worldwide, LLC v.*

*Liown Elecs. Co.*, 814 F.3d 1343, 1353 (Fed. Cir. 2016) (“We have found disavowal or disclaimer based on clear and unmistakable statements by the patentee that limit the claims, such as ‘the present invention includes . . .’ or ‘the present invention is . . .’ or ‘all embodiments of the present invention are . . .’”) (citation omitted). Here, we have repeated statements that “[t]he present invention is related to electronic communications systems and, more particularly, to communication using *incompatible* communication protocols.” (’588 Patent at 1:6-8. (emphasis added); *see also* ’588 Patent at 1:54-66; 2:22-27; 3:57-60; 4:10-13; 5:18-24.)

The ’588 Patent also makes clear that the interim / intermediate protocol is necessarily different from both the first and second protocols. For example, the ’588 Patent explains that the “interim protocol . . . *comprises the common functions and elements of the different protocols.*” (’588 Patent at 3:33-37 (emphasis added); *see also id.* at 2:10-12.) Thus, at least the uncommon aspects between the various expected communication protocols – *i.e.*, the first and second protocols – will make them different from the intermediate protocol, which reflects their commonalities.

FIG. 4 purportedly illustrates the conversion of a first protocol to an intermediate protocol via a first protocol table. (’588 Patent at FIG. 4, 5:44-58.) Likewise, FIG. 5 purportedly illustrates the conversion of an interim protocol to a second protocol via a second protocol table. (’588 Patent at FIG. 5, 5:59-6:10). No such conversions or tables would be necessary if the first or second protocol was identical to the intermediate protocol. And neither conversion table would be necessary if the first and second protocols are the same.

Accordingly, the Court should reject directPacket’s proposed construction of this term in favor of Polycom’s original construction as modified with the agreed construction of “protocol.”

2. **converting said first protocol into an intermediate protocol (claims 1, 11, 18) / convert said first protocol into an interim protocol using said**

**first protocol conversion table (claim 7)**

| <b><i>Polycom's Proposed Construction</i></b>  | <b><i>Plaintiff's Proposed Construction</i></b>   |
|--|---|
| <p>converting/convert the signaling portion of the first protocol into the signaling portion of an intermediate protocol, (claims 1, 7, 11, 18).</p> <p>A protocol is a set of conventions governing the format of messages exchanged between two communication devices, as set forth in the agreed-upon construction, <i>supra</i>.</p> | <p>creating messages, in real time, that are formatted according to an intermediate protocol from the multimedia data stream received in said first protocol, (claims 1, 11, 18).</p> <p>create messages, in real time, that are formatted according to an intermediate [sic] protocol from the multimedia data stream received in said first protocol using said first protocol conversion table, (claim 7).</p> |

The primary dispute between the parties is whether the “converting” recited in the ’588 Patent claims requires converting of the *signaling portion* of the first protocol into the *signaling portion* of the intermediate/interim protocol. Polycom’s proposed construction explicitly requires such conversion; while directPacket’s construction vaguely states that messages are created that are formatted according to an intermediate protocol, but provides no guidance as to what is actually being converted. The ’588 Patent specification and associated prosecution history make clear that only protocol messages and commands (*i.e.*, the signaling portion) of the incoming data stream, and not the payload or data portion, are what is converted.

During prosecution, Applicants repeatedly distinguished U.S. Patent No. 7,346,076 (“Habiby”) from the ’588 Patent, because Habiby merely discloses conversion of data (“bearer traffic”), but fails to disclose any conversion of the *signaling* information. (Ex. 7 at 14, 17, 18; Ex. 8 at 10-11.) Having made those arguments during prosecution, directPacket cannot now try to recover the scope it clearly disclaimed during prosecution. *Ekchian v. Home Depot, Inc.*, 104 F.3d 1299, 1304 (Fed. Cir. 1997) (“[S]ince, by distinguishing the claimed invention over the prior art, an applicant is indicating what the claims do not cover, he is by implication surrendering such protection.”) In particular, the Applicants stated “Thus, while Habiby

mentions conversion of its bearer traffic, it does NOT propose any conversion of the “signaling protocol” messages.” (Ex. 7 at 14; *see also* Ex. 8 at 10 (making the same arguments, verbatim); *see also* Ex. 7 at 17, 18.) The Applicants further extended their argument to ultimately claim that because Habiby’s bearer traffic is not a “signaling protocol,” Habiby does not disclose the claimed “converting” step of the ‘588 Patent, stating that “Habiby actually distinguishes its bearer traffic from the signaling protocols. That is, Habiby makes clear that the bearer traffic that it proposes converting is NOT a signaling protocol.” (Ex. 8 at 10-11; *see also* Ex. 9 at 12-13 (Applicant also argued that Ashar is distinguishable because that reference “does not teach or suggest converting a signaling protocol into an intermediate protocol.”).) Thus, by repeatedly distinguishing over the prior art because it does not teach conversion of a signaling protocol, the patentee’s statements show that the conversion required in the ‘588 Patent is of the signaling portion of the first protocol.

The above prosecution history statements are echoed in the specification of the ‘588 Patent. For example, the ‘588 Patent teaches that incoming data stream packets are “examin[ed] ... to find *protocol messages or commands* contained within the data stream. As such *protocol messages or commands* are found, protocol *converter* 201 accesses a corresponding table to find the *interim protocol message* to replace the *original message*,” thereby converting these original protocol messages or commands of the incoming data stream (*i.e.*, the *signaling portion* of the first protocol) to corresponding interim protocol messages or commands (*i.e.*, the *signaling portion* of the intermediate protocol). (‘588 Patent at 4:29-34 (emphasis added); *see also, id.* at 4:58-5:8; 4:41-51 (“Protocol converter 201 begins translating the data stream line by line into a new, interim data stream by retrieving the associated message or command in the interim

protocol from text table 203 and packaging the payload or data from the original data stream along with the message or command in the interim protocol”).) (Ex. 1 at ¶¶ 2-10).

Thus, the ’588 Patent expressly distinguishes between the protocol “*messages or commands*” (*i.e.*, the *signaling portion* of the protocol) and its *data portion* or *payload*, making clear that it is the signaling portion of first protocol that is being converted to that of an intermediate protocol, whereas the original data portion or payload remains unchanged and is merely repackaged with the converted signaling portion. (*See also, id.* at 5:9-18; 5:44-58, 5:59-6:10.; FIGs 4,5 (Ex. 1 at ¶¶ 2-10).)

The Court should reject directPacket’s improper importation of “real time” into the construction for “converting,” as none of the ’588 Patent claims recite any such limitation, nor does the specification clearly disclaim non real-time communications. *See Varco, L.P. v. Pason Sys. USA Corp.*, 436 F.3d 1368, 1372-1373 (Fed. Cir. 2006) (finding that it is the claims that delimit a patentee’s right to exclude, and therefore it is not proper to import limitations from the specification into the claims).

The protocols described in the specification are not limited to real-time operation. (Ex. 1 at ¶ 11. *see also* ’588 Patent at 1:28-30.) Those skilled in the art recognize that H.323 and SIP also allow for non-real-time communications, as do the TCP and UDP protocols discussed at col. 1, lines 31-39 of the ’588 Patent. (Ex. 1 at ¶ 11; ’978 Patent at 4:14-20, 5:57-62.)

Additionally, while the ’588 Patent discloses a single embodiment in which conversions may be performed in “real-time” by way of an “efficient interim protocol” (’588 Patent at 5:9-29), one of skill in the art would understand that such conversions need not be performed in “real-time” in accordance with other disclosed embodiments, such as in the computer system 600 depicted in FIG. 6. (Ex. 1 at ¶ 11.) For example, one of skill in the art would understand that

software to facilitate the claimed “converting” may be utilized in computer system 600 to allow a user to analyze, observe, or collect information about various protocol conversions by displaying timing diagrams, *e.g.*, via display adapter 609 and display 610, or generating reports via the display or a printer connected via I/O adapter 605, and the like. (’588 Patent at FIG. 6, 6:40-7:4; Ex. 1 at ¶ 12.) Accordingly, the ’588 Patent again contemplates that “converting” may be performed in non-real-time scenarios, as some such analysis, displaying, and reporting may not occur in “real time.” (Ex. 1 at ¶¶ 11-12.)

Because there is no clear disclaimer or limiting disclosure requiring that “converting” be performed in “real time,” the Court should reject directPacket’s construction.

**3. translating said intermediate protocol into a second protocol (claims 1, 11, 18)**

| <i>Polycom’s Proposed Construction</i>  | <i>Plaintiff’s Proposed Construction</i>   |
|---|--|
| <p>translating the signaling portion of said intermediate protocol into the signaling portion of a second protocol.</p> <p>A protocol is a set of conventions governing the format of messages exchanged between two communication devices, as set forth in the agreed-upon construction, <i>supra</i>.</p> | <p>creating messages, in real time, that are formatted according to a second protocol that is compatible with the target communication device from the multimedia data stream in the intermediate protocol</p> |

For the same reasons set forth in § V.A.2 *supra* with respect to the “converting” terms, the Court should adopt Polycom’s proposed construction for “translating.” In particular, there is no substantive difference between “converting” and “translating;” only the context in which they are used in the claims is different. The claims of the ’588 Patent use “converting” to indicate a change from a first protocol to an intermediate protocol, whereas “translating” is used to indicate a change from the intermediate protocol to a second protocol. (’588 Patent at claims 1, 11, 18) Accordingly, the Court should adopt Polycom’s construction for “translating.”

For the same reasons set forth in § V.A.2 *supra* with respect to the improper importation of “real time” in directPacket’s constructions for the “converting” terms, there is no clear disclaimer or limiting disclosure requiring that “translating” be performed in “real time.” Accordingly, the Court should reject directPacket’s construction for “translating” for at least this reason.

Contrary to directPacket’s construction, there is no language in independent claims 1, 11, or 18 that requires the “second protocol” to be “compatible with the target communication device.” (’588 Patent at Claims 1, 11, 18.) In fact, dependent claims 5, 15, and 22 each require retrieving exactly this type of “compatibility” information of the “second protocol” from a device information base. (’588 Patent at Claims 5, 15, 22.) Requiring the base independent claim to include a limitation of the dependent claim is improper. Moreover, importing such a limitation would exclude a preferred embodiment of the ’588 Patent, which too is improper. *On-Line Techs., Inc. v. Bodenseewerk Perkin-Elmer GmbH*, 386 F.3d 1133, 1138 (Fed. Cir. 2004). Specifically, the ’588 Patent discloses embodiments that include more than two prospective “target” endpoints. (’588 Patent, FIG. 1B (depicting prospective target endpoints 106, 107, 108, 109), 3:62-4:19.) For example, the ’588 Patent expressly states that “in additional and alternative embodiments of the present invention, ***any different type of communication protocol may be used by the various endpoints.*** Moreover, the communication controllers may be configured to service ***any number of different endpoints.***” (*Id.* at 3:57-61 (emphasis added).) Thus, in such embodiments, data may be destined for a plurality of “target endpoints” or “target communication devices,” whereby the recited “second protocol” need not be “compatible” with each such “target communication device,” as required by directPacket’s construction. That is, directPacket’s construction would exclude such embodiments, which is improper.



**B. U.S. Patent No. 7,710,978****1. commonly-open ('978 Patent: claims 1, 10, 11, 12, 14, 21, 22; '828 Patent: claims 9, 23)**

| <i>Polycom's Proposed Construction</i>   | <i>Plaintiff's Proposed Construction</i>        |
|--|---|
| Indefinite under 35 U.S.C. § 112.<br><br>Alternatively, if the Court finds "commonly-open" to be definite: open by default on most firewalls | any of the well-known ports or registered ports |

This term is indefinite because a person of ordinary skill would not understand how it could be satisfied. (Ex. 1 at ¶¶ 13-14.) *Nautilus, Inc. v. Biosig Instruments, Inc.* 572 U.S. 898, 910 (2014) (claims are indefinite where they fail to inform about the scope of the invention with reasonable certainty.) Those skilled in the art at issue in the '978 and '828 Patents would be unable to discern with reasonable certainty which ports are "commonly-open." If held not indefinite, the phrase should be construed as "open by default on most firewalls," which is the only criterion disclosed in the specification without contradictions elsewhere.

In Internet Protocol (IP) networks, applications or programs running on devices (or endpoints) on the network are identified by a "port" number. ('978 Patent at 1:30-33.) The ports may be blocked by a firewall to minimize the risk of allowing malicious traffic on the network. (*Id.* at 1:67-2:3.) When the port is blocked, it is "closed;" and when the port is not blocked, it is "open." (*Id.* at 2:17-30.) The patents define three types of ports: well-known ports (0-1023), registered ports (1024-49151) and dynamic/private ports (49152-65535).<sup>2</sup> (*Id.* at 1:33-50.)

The specification makes clear that the problem the '978 Patent is trying to solve is to allow firewalls to be traversed "*without changing any of their settings.*" ('978 Patent at Abstract.) For example, the '978 Patent expressly teaches away from changing or reconfiguring

---

<sup>2</sup> The numbers in the parentheses identify the range of ports available for each category.

settings such as firewall ports, explaining that “[r]econfiguring ports on a firewall is a time consuming task that introduces the risk of human error, which may defeat the purpose of the firewall by leaving a network vulnerable to malicious attacks.” (*Id.* at 2:23-30.) Instead, the ’978 Patent teaches that by “*choosing [a] ... commonly-open port* to communicate traffic through,” such reconfiguration will be avoided. (*Id.* at Abstract) (emphasis added.)

Though each of the asserted claims in the ’978 Patent and certain of the ’828 Patent claims recite “commonly-open ports,” this is not a term of art, and the patent specification does not clearly define which ports are commonly open. (Ex. 1 at ¶¶ 13-14.) The patent specification includes a variety of contradictory and ambiguous teachings about which subset of ports are “commonly-open.” Thus, one of ordinary skill in the art, reading the ’978 Patent and ’828 Patent (which incorporates the ’978 Patent specification (’828 Patent at 1:7-12)), is unable to determine whether a port is “commonly open” or not.

**a. ’978 Patent first asserts that only well-known ports (including port 443) are commonly-open, but registered and dynamic ports are not**

First, the ’978 Patent asserts that firewalls, especially those used by large corporations, generally only allow traffic from well-known ports and block all traffic on registered and dynamic ports (’978 Patent at 2:9-23). Accordingly, here, one of skill in the art would at best understand that while “well-known ports” may “generally” be commonly-open, registered and dynamic ports, in contrast, are “generally block[ed]” and not commonly-open.

Next, the ’978 Patent states that “travers[ing] a firewall by using a well-known port” ensures that “little or no reconfiguration of the firewall is required.” (’978 Patent at 3:10-13.) Here, one of skill in the art would at best understand that “well-known ports” may thus be commonly open.

In another example, the '978 Patent asserts that well-known port 443 is “commonly open by default on most firewalls (’978 Patent at 5:10-13.) Thus, here, one of skill in the art would understand that “well-known port 443” has the characteristic that it is commonly open by default on most firewalls.

**b. '978 Patent then disclaims its prior assertion that registered ports are generally blocked, and instead states that both well-known and registered ports are “typically open”**

Notwithstanding the teachings described above, the '978 Patent also disclaims its disclosure that registered ports will block traffic, *i.e.*, not be commonly-open, and instead states that registered ports may also be “typically open”:

The encapsulated packets are sent to device 24 using any of the well-known or registered ports, which are the ports that are typically open in standard firewalls.

(’978 Patent at 5:8-10.) Thus, reading the above statement in isolation, one of skill in the art would understand the '978 Patent to be teaching that both “well-known” and “registered ports” are commonly-open, contrary to the patent’s earlier disclosure.

**c. '978 Patent then disclaims even its *second* prior assertion, concluding that well-known ports, *certain registered ports*, and *the like on most firewalls in their standard configurations* are commonly-open**

Finally, the '978 Patent abandons its prior position and instead states that “most firewalls in their *standard configurations*” may have well-known ports, “certain” registered ports, “and the like” that are commonly open. What those “certain” registered ports or “and the like” ports are, much less what is meant by “firewalls in their *standard configurations*,” are left ambiguous and undisclosed:

While the packets may be sent along any of the well-known, registered, or dynamic ports, the preferable port used may be a port that is commonly open on *most firewalls* in their standard configurations (e.g., the well-known ports, *certain* registered ports, *and the like*).

(’978 Patent at 5:13-17 (emphasis added).) The specification gives no guidance about key criteria associated with this disclosure, such as: (1) which “certain” registered ports are “commonly open” (there are over 48,000 possible registered ports), (2) how many firewalls are sufficient to constitute “most firewalls,” and (3) which of the remaining ports are captured by the “*and the like*” teaching.

Thus, the ambiguous and contradictory teachings, including the catch-all “*and the like*” category, do not shed any light on which specific ports are “commonly-open.” Accordingly, one of skill in the art, looking at the ’978 and ’828 Patent specifications, would not understand the scope of what constitutes a “commonly-open” port and thus, would be unable to ascertain what meets the “commonly-open” limitation in the claims. (Ex. 1 at ¶¶ 13-14.)

**d. directPacket’s Proposed Construction is Expressly Refuted by the ’978 and ’828 Patent Specifications**

Notably, directPacket is unable to resolve the ambiguities created by the Patents’ disclosures, and is left to contend—contrary to the specifications—that “*any* of the well-known ports or registered ports” are “commonly open.” To the extent the Court deems that “commonly-open” is not indefinite and thus can be construed, directPacket’s proposed construction must be rejected, as it is expressly refuted by the ’978 and ’828 Patent specifications.

The specification expressly characterizes registered ports as being generally blocked, *i.e.*, not commonly-open. (’978 Patent at 2:9-23.) Elsewhere, the specification states that only “*certain* registered ports” are “commonly open on most firewalls in their standard configurations.” (’978 Patent at 5:13-17 (emphasis added).) Accordingly, the Court must reject directPacket’s construction requiring that “*any* of the well-known or registered ports” are commonly-open as the specification supports, at best, that well-known ports and only certain registered ports are commonly-open, and only for most firewalls in their standard configurations.

e. **If “commonly open” is found to be definite, then it should be construed as “open by default on most firewalls”**

To the extent the Court deems that “commonly-open” is definite and thus can be construed, Polycom’s proposed construction that “commonly-open” means “open by default on most firewalls” has explicit support in the specifications, and is not disclaimed or contradicted elsewhere in the Patents:

One such well-known port that could be chosen is port 443, which is commonly reserved for HTTPS traffic by ICANN and is ***commonly open by default on most firewalls***.

(’978 Patent at 5:10-13 (emphasis added).) Accordingly, the Court should adopt Polycom’s proposed construction, to the extent the Court deems “commonly-open” not indefinite.

2. **first /second [intermediate communication/network] device (claims 1, 14 of ‘978 Patent) first / second [intermediate communication / network] device (claims 1, 14 of ‘978 Patent)**

| <b><i>Polycom’s Proposed Construction</i></b>                              | <b><i>Plaintiff’s Proposed Construction</i></b>  |
|--|--|
| first and second devices that communicate with each other via the Internet | No construction necessary. Alternatively:<br><br>a [first/second] device that is logically disposed along a communication path between [a first/at least a first] endpoint communication device and [one or more other/at least a second] endpoint communication device[s] |

A patent claim term must be construed where a determination that a term ‘needs no construction’ would not resolve the parties’ dispute as to the scope of a claim. *Eon Corp. IP Holdings LLC v. Silver Spring Networks, Inc.*, 815 F.3d 1314, 1318 (Fed. Cir. 2016). As indicated by directPacket’s alternative proposed construction, the parties dispute the scope of this phrase, so it must be construed.

Polycom’s proposed construction is consistent with and limited to the disclosures of the patent. In contrast, directPacket’s proposed construction would expand the claims beyond what

the patent actually describes, and would thus be invalid for lack of written description. When construing a term, the construction should limit the scope of the claim term to that which is actually disclosed. *Ruckus Wireless, Inc. v. Innovative Wireless Solutions, LLC*, 824 F.3d 999, 1004 (Fed. Cir. 2016). It is a canon of claim construction that the court should construe claims to preserve their validity. *Id.*, citing *Gentry Gallery, Inc. v. Berkline Corp.*, 134 F.3d 1473, 1480 (Fed. Cir. 1998) (holding that a claim “may be no broader than the supporting disclosure”). Accordingly, directPacket’s proposed construction cannot be correct.

For example, the ’978 Patent teaches that if the endpoints are on the same network, the traffic does not need to pass through a firewall, and the need for its alleged invention is obviated. (’978 Patent at 6:47-54.) In other words, the patent teaches that network configuration in which the first and second intermediate communication devices are in a private network are outside the scope of the patent. But, such configurations are not outside of the scope of directPacket’s proposed construction, which must therefore be rejected.

The patent elaborates that the described encryption and firewall elements are only valuable if the communication between intermediate devices occurs over the Internet. (*See, e.g.*, ’978 Patent at 1:62-63, 2:31-34, 7:24-29.) In fact, more than merely describing the patented invention as advantageous when communicating over the Internet, the patent consistently contextualizes the invention as two systems communicating over the Internet. (*See e.g.*, ’978 Patent at 1:13-19, 4:37-38, and FIGs. 1-3.) Therefore, Polycom’s proposed construction requiring the first and second devices to communicate via the Internet should be adopted.

**3. multiport communication protocol (’978 Patent: 1, 6, 15; ’828 Patent: 1, 10, 11, 17)**

| <i>Polycom’s Proposed Construction</i>                 | <i>Plaintiff’s Proposed Construction</i>   |
|--|--|
| a protocol with packets destined for two or more ports | a protocol specifying media and control messages used in conducting real-time two- |

|  |  |
|--|--|
|  | way multimedia communication and communicated on two or more ports |
|--|--|

Polycom’s proposed construction is consistent with the claim language. *First*, the claims differentiate between “multiport communication protocol” and “single port communication protocol” and the parties agree that “multiport” means “two or more ports”. (*See e.g.*, ’978 Patent 8:52, 8:57-58.) *Second*, the claims each recite the receiving of “packets” in the multiport communication protocol. (’978 Patent at 8:49-54, 10:5-8; ’828 Patent at 13:65-14:3, 15:22-29; 16:34-38.) Thus, the claim language makes clear that a multiport communication protocol is a protocol with packets destined for two or more ports.

Polycom’s proposed construction is also consistent with the patents’ specifications, which make clear that multiport packets are destined for two or more ports. For example, FIG. 9 in the ’828 Patent depicts “multiport packets 900” as being destined for two or more ports 1010, 7040, and 50148-50153. (’828 Patent at 8:28, FIG. 9, *see also*, ’978 Patent at 5:2, FIG.2 (depicting “multiport packets 100” as being destined for a plurality of ports).) Likewise, the patent claims further confirm that “multiport packets” are destined for two or more ports, by reciting that such multiport packets are ultimately delivered to two or more ports. (’978 Patent at 9:6-10, 10:29-32, 12:4-7; ’828 Patent at 15:17-20, 15:36-40, 16:54-59.)

directPacket, on the other hand, seeks to insert a host of additional restrictions, including limiting the term to: (1) real-time communications, (2) two-way communications and (3) multimedia communications. None of these additional restrictions are justified from the intrinsic evidence. The specification makes clear that the multiple communication protocols described in the specification include both real-time and non-real-time communications. For example, the specification teaches that the H.323 and SIP protocols “typically allow for ... communication in real-time,” but does not disclaim non real-time scenarios. (’978 Patent at 1:26-29; Ex. 1 at ¶ 11.)

The specification also teaches that while some protocols like UDP are preferable for real-time communications, others such as TCP are preferred for communications requiring “data integrity,” whereby real-time communication is not possible. (’978 Patent at 4:14-18; Ex. 1 at ¶ 11.) The specification teaches that some protocols such as TCP are “at odds with maintaining real-time communication.” (’978 Patent at 5:57-62.) Thus, there is no disclaimer or limiting disclosure regarding the scope of the claimed protocols.

Similarly, the specification discloses both one-way and two-way communication. (’978 Patent at 5:45-50; ’828 Patent at 9:4-9.) (“While *one-way* communication is described . . . each of devices 21 and 24 may perform the steps of receiving multiple packets, encapsulation, port translation, decapsulation, and resending multiple packets in order to enable *two-way* communication....”), *see also* ’978 Patent at 4:42-44.) Accordingly, directPacket’s importation of a two-way communication limitation is improper and should be rejected.

While “multimedia communications traffic” is discussed in the specification (’978 Patent at 1:59-2:16), the specification does not limit the disclosure to multimedia protocols. To the contrary, the patent specification teaches that a “variety of protocols require the use of multiport traffic” including such non-media traffic as “data between applications,” and “control traffic.” (’978 Patent at 3:64-4:14.) Thus, the claims cannot be limited to multimedia communications.

4. **converting ... said plurality of multiport packets into a plurality of single-port packets in a single-port communication protocol (’978 Patent: 1; ’828 Patent: 1, 17); convert said plurality of multiport packets into a plurality of single-port packets in a single-port communication protocol (’978 Patent: 14); convert a plurality of multiport packets ... into a plurality of single-port packets in a single-port communication protocol (’828 Patent: 11)**

| <i>Polycom’s Proposed Construction</i>   | <i>Plaintiff’s Proposed Construction</i>  |
|--|---|
| converting packets destined for two or more ports into packets with a single destination port, (’978 Patent, claim 1, 14; ’828 Patent, | changing information in said plurality of packets in said multiport communication protocol, in real-time, and forming a plurality of packets in a |



|                    |  |
|--------------------|--|
| claims 1, 11, 17). | <p>single-port communication protocol, ('978 Patent, claim 1; '828 Patent, claims 1, 17).</p> <p>change information in said plurality of packets in said multiport communication protocol, in real-time, and form a plurality of packets in a single-port communication protocol, ('978 Patent, claim 14).</p> <p>change information in a plurality of packets in said multiport communication protocol, in real-time, and form a plurality of packets in a single-port communication protocol, ('828 Patent, claim 11).</p> |
|--------------------|--|

Polycom's proposed construction for the "converting" terms in the '978 and '828 Patents is consistent with the patent specifications and the claim language, both of which make clear that multiport packets are destined for two or more ports, and single-port packets have a single destination port. directPacket, on the other hand, seeks to insert additional restrictions, including limiting the term to real-time communications. Additional restrictions are not justified from the intrinsic evidence. (Ex. 1 at ¶ 11.) Accordingly, the Court should adopt Polycom's proposed construction.

The patent specifications make clear that multiport packets are destined for two or more ports. For example, FIG. 9 in the '828 Patent depicts "multiport packets 900" as being destined for two or more ports 1010, 7040, and 50148-50153. ('828 Patent at 8:28, FIG. 9; *see also* '978 Patent at 5:2, FIG.2 (depicting "multiport packets 100" as being destined for a plurality of ports).) Likewise, the patent claims further confirm that "multiport packets" are destined for two or more ports, by reciting that such multiport packets are ultimately delivered to two or more ports. ('978 Patent at 9:6-10, 10:29-32, 12:4-7; '828 Patent at 15:17-20, 15:36-40, 16:54-59.)<sup>3</sup>

---

<sup>3</sup> As explained in § V.B.3 *supra*, directPacket appears to agree that "multiport" means two or more ports, in view of its proposed construction for "multiport communication protocol."

The patent specifications also make clear that single-port packets have a single destination port. For example, FIG. 9 in the '828 Patent depicts "single-port packets 950" as having a single destination port. ('828 Patent at 8:28, FIG. 9. *See also*, '978 Patent at 5:2, FIG. 2 (depicting "single-port packets 200" having a single destination port).) Likewise, the patent claims further confirm that "single-port packets" have a single destination port, by reciting that such single-port packets are transmitted over a single so-called "commonly-open" port. ('978 Patent at 8:59-65, 10:15-18, 10:22-24, 11:23-34; '828 Patent at 15:4-8, 18:15-16.) Moreover, Applicants argued during prosecution that "the recitation of packets as being a plurality of 'single-port' packets merely reiterates that the packets are transmitted over a selected one of the plurality of different commonly-open ports...." (Ex. 6 at 12.)

For the same reasons set forth in § V.B.3 *supra*, there is no clear disclaimer or limiting disclosure requiring that "converting" be performed in "real time." Accordingly, the Court should reject directPacket's construction for "converting" for at least this reason.

5. **reconverting ... said received plurality of single-port packets into said multiport communication protocol ('978 Patent, claim 1; '828 Patent, claims 10, 17); reconverting said converted plurality of single-port packets into multiport communication protocol ('978 Patent, claim 14); reconvert said plurality of single-port packets into said multiport communication protocol ('828 Patent, claim 11)**

| <i>Polycom's Proposed Construction</i>   | <i>Plaintiff's Proposed Construction</i>  |
|--|---|
| reconverting packets with a single destination port into packets destined for two or more ports, whereby the resulting reconverted packets may differ in some way from the originally received multiport packets ('978 Patent, claims 1, 14; '828 Patent, claims 10, 11, 17) | changing information in said received plurality of single-port packets, in real time, and forming a plurality of packets in said multiport communication protocol, ('978 Patent, claim 1; '828 Patent, claims 10, 17).<br><br>changing information in said converted plurality of single-port packets, in real time, and forming a plurality of packets in said multiport communication protocol, ('978 Patent, claim 14).<br><br>change information in said plurality of single- |

|  |  |
|--|--|
|  | port packets, in real time, and form a plurality of packets in said multiport communication protocol, ('828 Patent, claim 11). |
|--|--|

Polycom's proposed construction for the "reconverting" terms in the '978 and '828 Patents is consistent with both the claim language and patent specifications, which make clear that multiport packets are destined for two or more ports, and single-port packets have a single destination port. (*See* §§ V.B.4, *supra*.)

Moreover, Applicants expressly argued during the prosecution of the '978 Patent that reconverting single-port packets to multiport packets "does not necessarily require that the resulting reconverted plurality of multiport packets be identical to the [originally received] multiport packets. ... Thus the resulting reconverted plurality of multiport packets may be identical to or may differ in some way (e.g., have additional information included therein, etc.) from the plurality of multiport packets that are recited as being received by a first intermediate communication device." (Ex. 6 at 9-10, 11, 14.) Polycom's proposed construction reflects this estoppel, whereas directPacket's does not.

Moreover, directPacket seeks to insert additional restrictions, including limiting the term to real-time communications. As explained in §§ V.B.3 *supra*, none of these additional restrictions are justified from the intrinsic evidence. (Ex. 1 at ¶ 11.) Therefore, the Court should adopt Polycom's proposed construction.

**C. U.S. Patent No. 8,560,828**

**1. external controller (claims 1, 2, 3, 4, 5, 11, 12, 13, 14, 15, 17, 18, 19)**

| <i>Polycom's Proposed Construction</i>    | <i>Plaintiff's Proposed Construction</i>   |
|---|--|
| a controller that resides in the Internet | No Construction Necessary;<br><br>Alternatively: a controller that is not behind [the recited firewall(s)] |

The parties' dispute regarding this term centers on the location of the claimed "external controller" relative to the remainder of the claimed system. *O2 Micro Int'l Ltd. v. Beyond Innovation Tech. Co.*, 521 F.3d 1351, 1362-63 (Fed. Cir. 2008) ("When the parties present a fundamental dispute regarding the scope of a claim term, it is the court's duty to resolve it.") In pertinent part, claim 1 of the '828 Patent reads:

Receiving at an external controller a communication request from said controller behind said firewall, **wherein said external controller is not behind said firewall**; ('828 Patent at Claim 1 (emphasis added)).

directPacket's proposed construction merely reads the bolded limitation into the construction of "external controller," and in so doing, fails to provide any clarity as to the meaning of the claim term at issue. The patent drafter attempted to clarify the modifier "external," by adding a wherein clause further specifying that the external controller is not behind the same firewall as the "said controller" from which it receives a communication request. This wherein clause ostensibly leaves open the possibility that the external controller is in the Internet or behind another firewall in another office. The "external controller," however, can't be behind another firewall in another office because that would be at odds with the plain meaning of the term "external" as the controller would be "internal" to the network of the remote office. Because the term could have multiple different meanings, a "plain and ordinary" construction, as proposed by directPacket, is inappropriate, *Eon Corp. IP Holdings LLC v. Silver Spring Network, Inc.*, 815 F.3d 1314, 1320 (Fed. Cir. 2016), and the Court should look to the specification and prosecution history to determine the appropriate scope of the claims. *Vitronics Corp. v. Conceptronic*, 90 F.3d 1576, 1582 (Fed. Cir. 1996).

During prosecution of the '828 Patent, Applicants explicitly identified front end controllers 410 of FIG. 4 and 804 and 806 of FIG. 8 as the claimed external controllers, each of which is depicted as resident only in the Internet. (Ex. 10 at 4-6; '828 Patent at FIGs. 4, 8.)

Similarly, FIG. 5 discloses front end controllers (*i.e.*, external controllers) as resident only in Internet 11. Thus, the only disclosures in the '828 Patent sufficient to enable the claims with respect to "external controller" consistently show that the external controller is located in the Internet. *Ruckus Wireless, Inc.*, 824 F.3d at 1004, citing *Gentry Gallery, Inc. v. Berkline Corp.*, 134 F.3d 1473, 1480 (Fed. Cir. 1998) (holding that a claim "may be no broader than the supporting disclosure.") Accordingly, the Court should construe "external controller" as a controller that resides in the Internet.

## 2. single endpoint communication device (claims 1, 10, 11)

| <i>Polycom's Proposed Construction</i> | <i>Plaintiff's Proposed Construction</i>  |
|--|---|
| only one endpoint communication device | No construction necessary. Alternatively:<br><br>at least one endpoint communication device |

The parties dispute whether "single endpoint communication device" is limited to only one endpoint communication device (Polycom) or may include multiple endpoint communication devices (directPacket). Because there is a dispute over the meaning of the phrase, the Court should construe the phrase. *O2 Micro Int'l Ltd. v. Beyond Innovation Tech. Co.*, 521 F.3d 1351, 1362-63 (Fed. Cir. 2008).

The claim language resolves the dispute in Polycom's favor. For example, claim 1 of the '828 Patent differentiates between a controller connected to "a plurality of endpoint communication devices" (meaning more than one) and a controller connected to "a single endpoint communication device." ('828 Patent at 13:65-67; 14:15-18 ("a controller . . . that is communicatively coupled with **a plurality** of endpoint communication devices" and "at least one other controller is configured to service **a single** endpoint communication device.")) Claim 10 makes the same distinction. (*Id.* at 15:22-23; 30-31 ("one or more shared controllers connected to **one or more** endpoint communication devices" and "individual controller connected to **a**

*single* endpoint communication device.”).) directPacket’s construction would vitiate the word “single” which is not proper. *Ad-In-The-Hole, International v. Hageman*, 1997 U.S. App. LEXIS 6213 at \*4 (Fed. Cir 1997) (“In construing a claim, we cannot ignore a limitation of the claim”) citing *Warner-Jenkinson Co. v. Hilton Davis Chemical Co.*, 520 U.S. 17, 29 (1997).

Other claim language gives further guidance about the meaning of “a *single* endpoint communication device.” Claim 4 recites a controller that communicates with “an additional endpoint communication device.” It is well settled that claims reciting “a” or “an” (as in claim 4) ordinarily mean “one or more.” However, in contrast to claim 4 of the ‘828 Patent, the additional modifier “single” in claim 1 indicates the inventor’s intention to limit the controller to service one and only one device. The Federal Circuit has previously ratified this precise distinction between “an” endpoint and “a single” endpoint. *Tate Access Floors v. Interface Architectural Res.*, 279 F.3d 1357, 1370 (Fed. Cir. 2002) (*holding* that “single visible decorative layer” was “clearly” meant to constrict the claim to one and only one particular layer.)

Polycom’s construction is also consistent with the specification, which differentiates between a controller that services multiple endpoint communication devices and one that is dedicated to only one endpoint communication device. For example, in summarizing the invention, the specification states that “there is at least one controller that services multiple endpoints and at least one controller that is *dedicated for a single endpoint*.” (*Id.* at 5:23-35 (emphasis added); *see also*, ’828 Patent at FIG 4). Thus, the Court should adopt Polycom’s proposed construction and limit the term to only one endpoint communication device.

## VI. CONCLUSION

For the foregoing reasons, Polycom’s respectfully requests that the Court adopt its proposed constructions for the identified terms in dispute.

Dated: July 2, 2019

Respectfully submitted,

/s/

---

Gary A. Bryant (VSB No. 27558)  
Jason E. Ohana (VSB No. 82485)  
Willcox & Savage, P.C.  
440 Monticello Avenue, Ste. 2200  
Norfolk, Virginia 23510  
757.628.5500  
757.628.5566 (facsimile)  
[gbryant@wilsav.com](mailto:gbryant@wilsav.com)  
[johana@wilsav.com](mailto:johana@wilsav.com)

Goutam Patnaik (*pro hac vice*)  
Tuhin Ganguly (*pro hac vice*)  
Ryan H. Ellis (VSB No. 89144)  
Pepper Hamilton LLP  
2000 K Street, N.W.  
Suite 600  
Washington, DC 20006-1865  
202.220.1200  
202.220.1465 (facsimile)  
[patnaikg@pepperlaw.com](mailto:patnaikg@pepperlaw.com)  
[gangulyt@pepperlaw.com](mailto:gangulyt@pepperlaw.com)  
[ellisr@pepperlaw.com](mailto:ellisr@pepperlaw.com)

Suparna Datta (*pro hac vice*)  
Brittanee L. Friedman (*pro hac vice*)  
Pepper Hamilton LLP  
19th Floor, High Street Tower  
125 High Street  
Boston, MA 02110 2736  
617.204.5100  
617.204.5150 (facsimile)  
[dattas@pepperlaw.com](mailto:dattas@pepperlaw.com)  
[friedmbr@pepperlaw.com](mailto:friedmbr@pepperlaw.com)

*Counsel for Defendant and Counter-Claimant  
Polycom, Inc.*

**CERTIFICATE OF SERVICE**

I hereby certify that on the 28th day of June, 2019, I will electronically file the foregoing with the Clerk of Court using the CM/ECF system, which will then send a notification of such filing to all counsel of record:

Christopher B. Ferenc, Esq.  
Terence P. Ross, Esq.  
Sean S. Wooden, Esq.  
Katten Muchin Rosenman LLP  
2900 K. Street NW, Ste. 200  
Washington, D.C. 20007-5118  
202.625.3500 Telephone  
202.339.6044 Facsimile  
christopher.ferenc@kattenlaw.com  
terence.ross@kattenlaw.com  
sean.wooden@kattenlaw.com

Yashas Kedar Honasoge, Esq.  
Katten Muchin Rosenman LLP  
525 W. Monroe St., Ste. 1600  
Chicago, Illinois 60661-3693  
312.902.5200 Telephone  
312.902.1061 Facsimile  
yashas.honasoge@kattenlaw.com

Stephen E. Noona, Esq.  
Kaufman & Canoles, P.C.  
150 W. Main St., Ste 2100  
Norfolk, Virginia 23510  
757.624.3239 Telephone  
888.360.9092 Facsimile  
senoona@kaufcan.com

*Counsel for Plaintiff*

/s/

---

Gary A. Bryant (VSB No. 27558)  
Jason E. Ohana (VSB No. 82485)  
Counsel for Polycom, Inc.  
Willcox & Savage, P.C.  
440 Monticello Ave., Ste. 2200  
Norfolk, Virginia 23510  
757.628.5500 Telephone  
757.628.5566 Facsimile  
gbryant@wilsav.com  
johana@wilsav.com



Goutam Patnaik (*pro hac vice*)  
Tuhin Ganguly (*pro hac vice*)  
Ryan H. Ellis (VSB No. 89144)  
Pepper Hamilton LLP  
2000 K Street, NW, Ste. 600  
Washington, DC 20006-1865  
202.220.1200 Telephone  
202.220.1465 Facsimile  
patnaikg@pepperlaw.com  
gangulyt@pepperlaw.com  
ellisr@pepperlaw.com

Suparna Datta (*pro hac vice*)  
Brittanee L. Friedman (*pro hac vice*)  
Pepper Hamilton LLP  
19th Floor, High Street Tower  
125 High Street  
Boston, MA 02110-2736  
617.204.5100 Telephone  
617.204.5150 Facsimile  
dattas@pepperlaw.com  
friedmbr@pepperlaw.com

*Counsel for Defendant  
and Counter-Claimant Polycom, Inc.*

# **EXHIBIT 1**

**IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA**

DIRECTPACKET RESEARCH, INC., Plaintiff,  
v.  
POLYCOM, INC., Defendant.

Civil Action No. 2:18-cv-00331-AWA-RJK

**DECLARATION OF TAL LAVIAN, PH.D.**

I, Tal Lavian, Ph.D., declare as follows:

**I. BACKGROUND AND QUALIFICATIONS**

1. I have been retained by Polycom, Inc. (“Polycom”) to provide expert opinion regarding the construction of certain claim terms in U.S. Patent Nos. 7,773,588, 7,710,978, and 8,560,828. The expert opinions set forth herein are based upon my knowledge in the field, review of the asserted patents, file histories, and information provided to me by counsel. Details of my background are set forth in my curriculum vitae, attached as Exhibit 1A to this Declaration.

**II. CONSTRUCTION OF TERMS IN THE ASSERTED PATENTS**

2. A protocol consists of a data/payload portion and a signaling/control portion. The data portion of a protocol is concerned with relaying the substance/content of interest to a software program/application. The signaling portion of a protocol specifies, for example, (i) the location for which the data is destined, and from which it originates; (ii) the particular format or encoding of the data; (iii) details about when the data should be transferred; and (iv) any other details that may be necessary for managing the data portion. Each of these pieces of discrete signaling information are commands, or messages to the software application(s), about how to handle the data portion.

3. The data portion of a protocol normally handles a higher volume of data than the signaling portion. That is, the data portion of a protocol handles the “what,” while the signaling portion handles the “how.” In other words, the data portion of a protocol consists of the actual flow of application-level data, while the signaling portion controls or directs that flow. Automobile traffic

within a city provides an analogy: the automobiles are analogous to the data portion, while the traffic lights, stop signs, detour signs, crossing guards, etc. are analogous to the signaling portion.

4. In telecommunications, a multimedia-communication protocol similarly includes a data portion and a signaling portion. Most commonly, the data portion is handled by RTP. For the signaling portion, there are at least two common choices: SIP and H.323. The '588 Patent specifically and repeatedly describes SIP and H.323, how they are different (e.g., SIP is text-based, while H.323 is binary-coded), and how a need arises to convert one to the other. The '588 Patent does not mention RTP or any other data portion. Thus, one of skill in the art would understand that the '588 Patent aims to solve the conversion/translation problem between the signaling portions, such as SIP and H.323, of multimedia-communication protocols.

5. Referring to the automobile-traffic analogy described in ¶ 3 *supra*, a driver crossing a border between countries would have to quickly familiarize himself with the conventions in the new country: the language and/or shapes of street signs, the positioning of traffic lights, etc. But it is rare that the automobile itself would need to actually change in some way when it crosses a border.

6. In some protocols, the signaling portion and data portion can co-exist within the same information stream. To use another analogy, a telephone conversation between two people typically consists of a signaling portion and a data portion. The signaling portion is performed according to standard conventions. For example, each person greets the other with “hello” at the beginning of the call, confirms the other person’s identity, verifies that the other is able to talk, and so on. Then, the substantive conversation begins – this is the data portion of the call. Finally, before ending the call, both parties will acknowledge that they are ready to end the conversation (e.g. “goodbye”). Such end-of-conversation acknowledgment is more signaling information: it is used to control the conversation itself.

7. The '588 Patent teaches that messages or commands – i.e., the signaling portion of the multimedia data stream are converted, *not* the data or payload.

8. The '588 Patent explains that a “protocol convertor” begins “examining the data stream packet to find protocol messages or commands contained within the data stream.” ('588 Patent at 4:20-34, FIG. 2.) The data stream includes both (i) the actual content or substance of the multimedia data stream – i.e., the “data” or “payload” portion; and (ii) the “protocol messages or commands” – i.e., the “signaling” portion.” The protocol convertor 201 replaces the “protocol message” format from one protocol to another via the protocol tables (e.g., “Binary Table 202” or “Text Table 203”). ('588 Patent at FIG. 2.) Thus, I understand that messages or commands – i.e., the signaling portion of the multimedia data stream – are converted, *not* the data or payload portion.

9. FIG. 4 (element 401) of the '588 Patent depicts the step of “select[ing] interim protocol messages from the table.” Here, selecting a protocol message from a table can only mean that signaling messages and commands are being selected from the multimedia data stream, and not any portion of the payload. Selecting from a table is only possible when limited to predefined protocol messages. It would be impossible to select the actual payload from a table, because the actual payload or content of the multimedia data stream is unknown to the protocol.

10. The '588 Patent's disclosure that “protocol messages or commands” are being converted must necessarily mean that signaling information is what is being converted. The data or payload portion of “the multimedia data stream” cannot be known to the protocol in advance of the transmitting of the data/payload itself. Moreover, the data/payload portion cannot even be converted based on the invention described. A person of skill in the art would know that it is not possible to implement the purported '588 Patent invention to convert the infinite possibilities of payload *data* messages via a table lookup. A table must have a finite size; whereas the scope of possibilities of the actual payload data messages of a multimedia data stream is infinitely large.

11. **TCP/UDP.** Internet communication is based on the TCP and UDP protocols. TCP tracks sent and received packets by an acknowledgment (ACK) mechanism. UDP does not use acknowledgments at all, and is usually used for applications that do not care if some packets are lost in transmission. TCP is considered a reliable data-transfer protocol, and it confirms that the application receives all data in the order transmitted. UDP protocol does not care if packets arrived at all, and lost or out-of-order packets are acceptable. Thus, a person of skill in the art would understand that UDP is well-suited for real-time communications, whereas TCP is well-suited for communications that can tolerate latencies necessary to ensure data integrity.

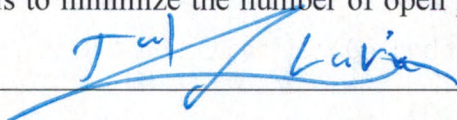
12. For example, a person of skill in the art would understand that the system shown in FIG. 6 of '588 Patent could use the '588 Patent invention (e.g., the software code that does all the claimed steps) in a non-real time situation – e.g., to analyze, observe, or collect information about various protocol conversions by displaying timing diagrams – e.g., via display adapter 609 and display 610, or by generating reports via the display or a printer connected via I/O adapter 605, and the like.

13. **commonly-open.** The term “commonly-open” port is not a term of art. Having read the '978 and '828 Patents and their file histories, it is my opinion that one of skill in the art would not understand the scope of what would or would not constitute a “commonly-open” port.

14. To the extent the Court requires the term “commonly-open” to be construed, I agree with Polycom that the construction “open by default on most firewalls” has explicit support in the '978 and '828 Patent specifications, and is not disclaimed or contradicted elsewhere in these Patents.

Plaintiff directPacket's proposed construction stating that “any of the well-known ports or registered ports” are commonly-open cannot be correct. If all well-known and registered ports were open, the principal goal of the '978 Patent, which is to minimize the number of open ports, would be subverted.

Dated: July 2, 2019

  
\_\_\_\_\_  
Tal Lavian, Ph.D.

# **EXHIBIT 1A**

## Dr. Tal Lavian



<https://TelecommNet.com>  
[tlavian@TelecommNet.com](mailto:tlavian@TelecommNet.com)



1640 Mariani Dr.  
Sunnyvale, CA 94087  
(408)-209-9112

## Telecommunications, Network Communications and Mobile Wireless Technologies Expert

Scientist, educator, and technologist with 30 years of experience. He has co-authored over 25 scientific publications, journal articles, and peer-reviewed papers. Dr. Lavian serves as an expert in network communications, telecommunications, Internet protocols, and mobile wireless technologies. He is the named inventor of over 120 issued and filed patents. He served as Principal Investigator (PI) for three US Department of Defense (DARPA) projects.

### EDUCATION

- **Ph.D.**, Computer Science specializing in networking and communications, UC Berkeley
- **M.Sc.**, Electrical Engineering, Tel Aviv University
- **B.Sc.**, Mathematics and Computer Science, Tel Aviv University

### EXPERTISE

Network communications, telecommunications, Internet protocols, and mobile wireless:

- **Communication networks:** Internet protocols; TCP/IP suite, TCP, UDP, IP, Ethernet, 802.3, network protocols, network software applications, data link, network, and transport layers (L2, L3, L4), packet switching, data center network architecture
- **Mobile wireless:** Wi-Fi, 802.11 (a/b/g/n/ac), Bluetooth, MAC, PHY, OFDM, DSSS, Wireless LAN (WLAN). Cellular systems, GSM, LTE, CDMA, FDMA, TDMA, SMS, instant messaging (chat), mobile devices, smartphone
- **Internet/cloud:** Web applications, HTTP, e-mail, SMTP, POP, IMAP, Java, C/C++, file transfer FTP, client-server, cloud computing, distributed computing
- **Routing/switching:** LAN, WAN, VPN, routing protocols, RIP, BGP, MPLS, OSPF, multicast, DNS, QoS, network infrastructure, network communication architectures
- **Unified Communications:** PSTN, circuit switching, IP telephony, VoIP, SIP, RTP, SS7, optical networks, carrier Ethernet, SONET, SDH, WDM, TDM, video/audio conferencing, streaming media

### ACCOMPLISHMENTS

- Served as Principal Investigator (PI) for three US Department of Defense (DARPA) projects
  - Directed networking computation project for the US Air Force Research Lab (AFRL)
  - PI of a wireless research project for an undisclosed US federal agency
- Led and developed the first network resource scheduling service for grid computing
- Managed and engineered the first demonstrated transatlantic dynamic allocation of 10Gbs Lambdas as a grid service
- Development and successful demonstration of the first wire-speed active network on commercial hardware



- Inventor of over 120 patents, over 60 prosecuted *pro se* in front of the USPTO
- Created and chaired Nortel Networks' EDN Patent Committee

## PROFESSIONAL EXPERIENCE

**University of California, Berkeley,** Berkeley, California 2000-Present  
**UC Berkeley SkyDeck, Industry Fellow, Lecturer, Visiting Scientist, Ph.D. Candidate, Nortel's Scientist Liaison**

*Some positions and projects were concurrent, others sequential*

- UC Berkeley SkyDeck startups - advanced technology research, development, business, and market
- Industry fellow and lecturer at the Sutardja Center for Entrepreneurship and Technology (SCET).
- Conducted research projects in data centers (RAD Labs), telecommunication infrastructure (SAHARA), and wireless systems (ICEBERG)
- Acted as scientific liaison between Nortel Research Lab and UC Berkeley, providing tangible value in advanced technologies
- Developed long-term technology for the enterprise market, integrating communication and computing technologies
- Studied network services, telecommunication systems and software, communications infrastructure, and data centers
- Earned a Ph.D. in Computer Science with a specialization in communications and networking

**TelecommNet Consulting, Inc.** Sunnyvale, California 2006-Present  
**Principal Scientist**

- Consulting in the areas of network communications, telecommunications, Internet protocols, and smartphone mobile wireless devices
- Providing system architecture and technology analysis for computer networks, mobile wireless devices, and Internet web technologies projects
- Providing expert witness services in network communications patent infringement lawsuits

**CRadar.Ai,** UC Berkeley, California 2018-Present  
**Principal Investigator**

- CRadar.Ai improves the Radar wireless RF signal phase noise purity by 100x
- Accurate Radars are paramount for self-driving car safety. Radars "see" where Cameras and LiDars are "blind" (fog, rain, snow, direct sunlight, and darkness)
- The superior wireless RF signal quality provides clean signal for high Radar accuracy
- Improving Radar accuracy and resolution enables true redundancy, sensory fusion and puts the Radar into the sensory spearhead

**Aybell (VisuMenu Inc.),** UC Berkeley, California 2016-Present  
**CEO/CTO**

- Aybell transforms smartphones into visual menu systems, making the phone a frictionless point for user interactions with all features of customer service platforms. Empowers consumers to reach the right agents in call centers, overcoming customer service barriers. Aybell is a branding and marketing of VisuMenu advanced technologies.

- Architecture, design and implementation of a cloud data center for connecting any smartphone user, to any company and/or service, by digitizing interactive voice systems, and exposing through cloud-service APIs to other applications
- The system is deployed as a cloud networking and cloud computing service on Amazon Web Services (AWS) and Google Cloud Platform (GCP)
- Technologies include Data Science analytics, Machine Learning (ML), Artificial Intelligence (AI), and Statistical Learning (SL). Building an NLP Parser using Python, NLTK, SpaCy and other NLP libraries and modules

**VisuMenu, Inc.**, Sunnyvale, California

2010-2016

**Co- Founder and Chief Technology Officer (CTO)**

- Led the software design and development of a visual IVR system for smartphones and mobile devices, based on an innovative use of wireless and network communications technologies
- Design of a search engine for IVR / PBX using Asterisk, SIP, and VoIP
- The system was deployed as a cloud networking and cloud computing service on Amazon Web Services (AWS) and Google Cloud Platform (GCP).
- VisuMenu advanced technologies rebranded as Aybell.

**Ixia**, Santa Clara, California

2008 - 2008

**Communications Consultant**

- Researched and developed advanced network communications testing technologies:
- IxNetwork/IxN2X —IP routing and switching devices and broadband access equipment. Provided traffic generation and emulation for the full range of protocols: OSPF, RIP, EIGRP, BGP, IS-IS, MPLS, unicast, multicast, broadcast, layer 2/3 VPNs, IPsec, carrier Ethernet, broadband access, and data center bridging. Tested and validated IEEE, ITU and IETF RFC standards compatibility
- IxLoad — quickly and accurately modeled high-volume video, data, and voice subscribers and servers to test real-world performance of multiservice delivery and security platforms
- IxCatapult — emulated a broad range of wireless access and core protocols to test wireless components and systems that, when combined with IxLoad, provides an end-to-end solution for testing wireless service quality
- IxVeriWave — employed a client-centric model to test Wi-Fi and wireless LAN networks by generating repeatable large-scale, real-world test scenarios that are virtually impossible to create by any other means
- Test automation — provided simple, comprehensive lab automation to help test engineering teams create, organize, catalog, and schedule execution of tests

**Nortel Networks**, Santa Clara, California

1996 - 2007

*Originally employed by Bay Networks, which was acquired by Nortel Networks*

**Principal Scientist, Principal Architect, Principal Engineer, Senior Software Engineer**

*Held scientific and research roles at Nortel Labs, Bay Architecture Labs, and in the office of the CTO*

**Principal Investigator for US Department of Defense (DARPA) Projects**

- Conceived, proposed, and completed three research projects: active networks, DWDM-RAM, and a networking computation project for Air Force Research Lab (AFRL)
- Led a wireless research project for an undisclosed US federal agency

### **Academic and Industrial Researcher**

- Analyzed new technologies to reduce risks associated with R&D investment
- Headed research collaboration with leading universities and professors at UC Berkeley, Northwestern University, University of Amsterdam, and University of Technology, Sydney
- Evaluated competitive products relative to Nortel's products and technology
- Proactively identified prospective business ideas, which led to new networking products
- Predicted technological trends through researching the technological horizon and academic sphere
- Designed software for switches, routers, and network communications devices
- Developed systems and architectures for switches, routers, and network management
- Researched and developed the following projects:
 

|  |           |
|--|-----------|
| ▪ Data-Center Communications: network and server orchestration           | 2006-2007 |
| ▪ DRAC: SOA-facilitated L1/L2/L3 network dynamic controller              | 2003-2007 |
| ▪ Omega: classified wireless project for undisclosed US Federal Agency   | 2006-2006 |
| ▪ Open platform: project for the US Air Force Research Laboratory (AFRL) | 2005-2005 |
| ▪ Network resource orchestration for Web services workflows              | 2004-2005 |
| ▪ Proxy study between Web/grids services and network services            | 2004-2004 |
| ▪ Streaming content replication: real-time A/V media multicast at edge   | 2003-2004 |
| ▪ DWDM-RAM: US DARPA-funded program on agile optical transport           | 2003-2004 |
| ▪ Packet capturing and forwarding service on IP and Ethernet traffic     | 2002-2003 |
| ▪ CO2: content-aware agile networking                                    | 2001-2003 |
| ▪ Active networks: US DARPA-funded research program                      | 1999-2002 |
| ▪ ORE: programmable network service platform                             | 1998-2002 |
| ▪ JVM platform: Java on network devices                                  | 1998-2001 |
| ▪ Web-based device management: network device management                 | 1996-1997 |

### **Technology Innovator and Patent Leader**

- Created and chaired Nortel Networks' EDN Patent Committee
- Facilitated continuous stream of innovative ideas and their conversion into intellectual property rights
- Developed intellectual property assets through invention and analysis of existing technology portfolios

**Aptel Communications**, Netanya, Israel 1994-1995

#### **Software Engineer, Team Leader**

*Start-up company focused on mobile wireless CDMA spread spectrum PCN/PCS*

- Developed a mobile wireless device using an unlicensed band - Direct Sequence Spread Spectrum (DSSS); FCC part 15 - unlicensed transmitters
- Designed and managed a personal communication network (PCN) and personal communication system (PCS), which were the precursors of short text messages (SMS)
- Designed and developed network communications software products in C/C++
- Invented and implemented a two-way paging product

**Scitex Ltd.**, Herzeliya, Israel 1990-1993

#### **Software Engineer, Team Leader**

*Software and hardware company acquired by Hewlett Packard (HP)*

- Developed system and network communications in C/C++

- Invented Parallel SIMD Architecture
- Participated in the Technology Innovation group

**Shalev**, Ramat-HaSharon, Israel

1987-1990

*Start-up company*

**Software Engineer**

- Developed real-time software and algorithms in C/C++ and Pascal

**PROFESSIONAL ASSOCIATIONS**

- IEEE senior member
- IEEE CNSV co-chair, Intellectual Property SIG (2013)
- President Next Step Toastmasters (an advanced TM club in the Silicon Valley) (2013-2014)
- Technical co-chair, IEEE Hot Interconnects 2005 at Stanford University
- Member, IEEE Communications Society (COMMSOC)
- Member, IEEE Computer Society
- Member, IEEE Systems, Man, and Cybernetics Society
- Member, IEEE-USA Intellectual Property Committee (2012)
- Member, ACM, ACM Special Interest Group on Data Communication (SIGCOM)
- Member, ACM Special Interest Group on Hypertext, Hypermedia, and Web (SIGWEB)
- Member, IEEE Consultants' Network (CNSV)
- Global Member, Internet Society (ISOC)
- President Java Users Group – Silicon Valley Mountain View, CA, 1999-2000
- Toastmasters International

**FORMER ADVISORY BOARDS POSITIONS**

- Quixey – search engine for wireless mobile apps
- Mytopia – mobile wireless social games
- iLeverage – Israeli Innovations

**PROFESSIONAL AWARDS**

- Top Talent Award – Nortel
- Top Inventors Award – Nortel EDN
- Certified IEEE-WCET - Wireless Communications Engineering Technologies (2012)
- Toastmasters International - Competent Communicator (twice)
- Toastmasters International - Advanced Communicator Bronze

**PERSONAL**

- USA FIT – San Jose Marathon running club (2017-2018-2019)
- Hiking Bateva – hiking club
- A dancer for 45 years

## Patents and Publications

*(Not an exhaustive list)*

### Patents Issued

|                                     |   |                             |
|-------------------------------------|---|-----------------------------|
| <a href="#"><u>US 9,831,881</u></a> | <a href="#"><u>Radar target detection system for autonomous vehicles with ultra-low phase noise frequency synthesizer</u></a> | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 9,762,251</u></a> | <a href="#"><u>Ultra-low phase noise frequency synthesizer</u></a>  | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 9,705,511</u></a> | <a href="#"><u>Ultra-low phase noise frequency synthesizer</u></a>  | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 9,690,877</u></a> | <a href="#"><u>Systems and methods for electronic communications</u></a>  | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 9,660,655</u></a> | <a href="#"><u>Ultra-low phase noise frequency synthesizer</u></a>  | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 9,184,989</u></a> | <a href="#"><u>Grid proxy architecture for network resources</u></a>  | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 9,521,255</u></a> | <a href="#"><u>Systems and methods for visual presentation and selection of IVR menu</u></a>                                  | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 9,083,728</u></a> | <a href="#"><u>Systems and methods to support sharing and exchanging in a network</u></a>                                     | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 9,021,130</u></a> | <a href="#"><u>Photonic line sharing for high-speed routers</u></a>   | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 9,001,819</u></a> | <a href="#"><u>Systems and methods for visual presentation and selection of IVR menu</u></a>                                  | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 8,949,846</u></a> | <a href="#"><u>Time-value curves to provide dynamic QoS for time sensitive file transfers</u></a>                             | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 8,929,517</u></a> | <a href="#"><u>Systems and methods for visual presentation and selection of IVR menu</u></a>                                  | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 8,903,073</u></a> | <a href="#"><u>Systems and methods for visual presentation and selection of IVR menu</u></a>                                  | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 8,898,274</u></a> | <a href="#"><u>Grid proxy architecture for network resources</u></a>  | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 8,880,120</u></a> | <a href="#"><u>Device and method for providing enhanced telephony</u></a>   | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 8,879,703</u></a> | <a href="#"><u>System method and device for providing tailored services when call is on-hold</u></a>                          | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 8,879,698</u></a> | <a href="#"><u>Device and method for providing enhanced telephony</u></a>   | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 8,867,708</u></a> | <a href="#"><u>Systems and methods for visual presentation and selection of IVR menu</u></a>                                  | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 8,787,536</u></a> | <a href="#"><u>Systems and methods for communicating with an interactive voice response system</u></a>                        | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 8,782,230</u></a> | <a href="#"><u>Method and apparatus for using a command design pattern to access and configure network elements</u></a>       | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 8,762,963</u></a> | <a href="#"><u>Translation of programming code</u></a>  | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 8,762,962</u></a> | <a href="#"><u>Methods and apparatus for automatic translation of a computer program language code</u></a>                    | <a href="#"><u>Link</u></a> |

|                                     |   |                             |
|-------------------------------------|---|-----------------------------|
| <a href="#"><u>US 8,745,573</u></a> | <a href="#"><u>Platform-independent application development framework</u></a>   | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 8,731,148</u></a> | <a href="#"><u>Systems and methods for visual presentation and selection of IVR menu</u></a>  | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 8,688,796</u></a> | <a href="#"><u>Rating system for determining whether to accept or reject objection raised by user in social network</u></a>           | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 8,619,793</u></a> | <a href="#"><u>Dynamic assignment of traffic classes to a priority queue in a packet forwarding device</u></a>                        | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 8,572,303</u></a> | <a href="#"><u>Portable universal communication device</u></a>  | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 8,553,859</u></a> | <a href="#"><u>Device and method for providing enhanced telephony</u></a>   | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 8,548,131</u></a> | <a href="#"><u>Systems and methods for communicating with an interactive voice response system</u></a>                                | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 8,537,989</u></a> | <a href="#"><u>Device and method for providing enhanced telephony</u></a>   | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 8,341,257</u></a> | <a href="#"><u>Grid proxy architecture for network resources</u></a>  | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 8,161,139</u></a> | <a href="#"><u>Method and apparatus for intelligent management of a network element</u></a>   | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 8,146,090</u></a> | <a href="#"><u>Time-value curves to provide dynamic QoS for time sensitive file transfer</u></a>                                      | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 8,078,708</u></a> | <a href="#"><u>Grid proxy architecture for network resources</u></a>  | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 7,944,827</u></a> | <a href="#"><u>Content-aware dynamic network resource allocation</u></a>  | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 7,860,999</u></a> | <a href="#"><u>Distributed computation in network devices</u></a>   | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 7,734,748</u></a> | <a href="#"><u>Method and apparatus for intelligent management of a network element</u></a>   | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 7,710,871</u></a> | <a href="#"><u>Dynamic assignment of traffic classes to a priority queue in a packet forwarding device</u></a>                        | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 7,580,349</u></a> | <a href="#"><u>Content-aware dynamic network resource allocation</u></a>  | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 7,433,941</u></a> | <a href="#"><u>Method and apparatus for accessing network information on a network device</u></a>                                     | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 7,359,993</u></a> | <a href="#"><u>Method and apparatus for interfacing external resources with a network element</u></a>                                 | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 7,313,608</u></a> | <a href="#"><u>Method and apparatus for using documents written in a markup language to access and configure network elements</u></a> | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 7,260,621</u></a> | <a href="#"><u>Object-oriented network management interface</u></a>   | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 7,237,012</u></a> | <a href="#"><u>Method and apparatus for classifying Java remote method invocation transport traffic</u></a>                           | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 7,127,526</u></a> | <a href="#"><u>Method and apparatus for dynamically loading and managing software services on a network device</u></a>                | <a href="#"><u>Link</u></a> |

|                                     |  |                             |
|-------------------------------------|--|-----------------------------|
| <a href="#"><u>US 7,047,536</u></a> | <a href="#"><u>Method and apparatus for classifying remote procedure call transport traffic</u></a>  | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 7,039,724</u></a> | <a href="#"><u>Programmable command-line interface API for managing operation of a network device</u></a>  | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 6,976,054</u></a> | <a href="#"><u>Method and system for accessing low-level resources in a network device</u></a>   | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 6,970,943</u></a> | <a href="#"><u>Routing architecture including a compute plane configured for high-speed processing of packets to provide application layer support</u></a> | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 6,950,932</u></a> | <a href="#"><u>Security association mediator for Java-enabled devices</u></a>  | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 6,850,989</u></a> | <a href="#"><u>Method and apparatus for automatically configuring a network switch</u></a>   | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 6,845,397</u></a> | <a href="#"><u>Interface method and system for accessing inner layers of a network protocol</u></a>  | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 6,842,781</u></a> | <a href="#"><u>Download and processing of a network management application on a network device</u></a>   | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 6,772,205</u></a> | <a href="#"><u>Executing applications on a target network device using a proxy network device</u></a>  | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 6,564,325</u></a> | <a href="#"><u>Method of and apparatus for providing multi-level security access to system</u></a>   | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 6,175,868</u></a> | <a href="#"><u>Method and apparatus for automatically configuring a network switch</u></a>   | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 6,170,015</u></a> | <a href="#"><u>Network apparatus with Java co-processor</u></a>  | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 8,687,777</u></a> | <a href="#"><u>Systems and methods for visual presentation and selection of IVR menu</u></a>   | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 8,681,951</u></a> | <a href="#"><u>Systems and methods for visual presentation and selection of IVR menu</u></a>   | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 8,625,756</u></a> | <a href="#"><u>Systems and methods for visual presentation and selection of IVR menu</u></a>   | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 8,594,280</u></a> | <a href="#"><u>Systems and methods for visual presentation and selection of IVR menu</u></a>   | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 8,548,135</u></a> | <a href="#"><u>Systems and methods for visual presentation and selection of IVR menu</u></a>   | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 8,406,388</u></a> | <a href="#"><u>Systems and methods for visual presentation and selection of IVR menu</u></a>   | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 8,345,835</u></a> | <a href="#"><u>Systems and methods for visual presentation and selection of IVR menu</u></a>   | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 8,223,931</u></a> | <a href="#"><u>Systems and methods for visual presentation and selection of IVR menu</u></a>   | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 8,160,215</u></a> | <a href="#"><u>Systems and methods for visual presentation and selection of IVR menu</u></a>   | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 8,155,280</u></a> | <a href="#"><u>Systems and methods for visual presentation and selection of IVR menu</u></a>   | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 8,054,952</u></a> | <a href="#"><u>Systems and methods for visual presentation and selection of IVR menu</u></a>   | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 8,000,454</u></a> | <a href="#"><u>Systems and methods for visual presentation and selection of IVR menu</u></a>   | <a href="#"><u>Link</u></a> |
| <a href="#"><u>EP 1,905,211</u></a> | <a href="#"><u>Technique for authenticating network users</u></a>  | <a href="#"><u>Link</u></a> |

|                                     |  |                             |
|-------------------------------------|--|-----------------------------|
| <a href="#"><u>EP 1,142,213</u></a> | <a href="#"><u>Dynamic assignment of traffic classes to a priority queue in a packet forwarding device</u></a> | <a href="#"><u>Link</u></a> |
| <a href="#"><u>EP 1,671,460</u></a> | <a href="#"><u>Method and apparatus for scheduling resources on a switched underlay network</u></a>            | <a href="#"><u>Link</u></a> |
| <a href="#"><u>CA 2,358,525</u></a> | <a href="#"><u>Dynamic assignment of traffic classes to a priority queue in a packet forwarding device</u></a> | <a href="#"><u>Link</u></a> |
| <a href="#"><u>CA 2,989,752</u></a> | <a href="#"><u>Ultra-low Phase Noise Frequency Synthesizer</u></a>   | <a href="#"><u>Link</u></a> |



**Patent Applications Published and Pending***(Not an exhaustive list)*

|                                       |   |                             |
|---------------------------------------|---|-----------------------------|
| <a href="#"><u>US 20150058490</u></a> | <a href="#"><u>Grid Proxy Architecture for Network Resources</u></a>  | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20150010136</u></a> | <a href="#"><u>Systems and Methods for Visual Presentation and Selection of IVR Menu</u></a>                            | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20140379784</u></a> | <a href="#"><u>Method and Apparatus for Using a Command Design Pattern to Access and Configure Network Elements</u></a> | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20140105025</u></a> | <a href="#"><u>Dynamic Assignment of Traffic Classes to a Priority Queue in a Packet Forwarding Device</u></a>          | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20140105012</u></a> | <a href="#"><u>Dynamic Assignment of Traffic Classes to a Priority Queue in a Packet Forwarding Device</u></a>          | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20140012991</u></a> | <a href="#"><u>Grid Proxy Architecture for Network Resources</u></a>  | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20130080898</u></a> | <a href="#"><u>Systems and Methods for Electronic Communications</u></a>  | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20130022191</u></a> | <a href="#"><u>Systems and Methods for Visual Presentation and Selection of IVR Menu</u></a>                            | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20130022183</u></a> | <a href="#"><u>Systems and Methods for Visual Presentation and Selection of IVR Menu</u></a>                            | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20130022181</u></a> | <a href="#"><u>Systems and Methods for Visual Presentation and Selection of IVR Menu</u></a>                            | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20120180059</u></a> | <a href="#"><u>Time-Value Curves to Provide Dynamic QOS for Time Sensitive File Transfers</u></a>                       | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20120063574</u></a> | <a href="#"><u>Systems and Methods for Visual Presentation and Selection of IVR Menu</u></a>                            | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20110225330</u></a> | <a href="#"><u>Portable Universal Communication Device</u></a>  | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20100220616</u></a> | <a href="#"><u>Optimizing Network Connections</u></a>   | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20100217854</u></a> | <a href="#"><u>Method and Apparatus for Intelligent Management of a Network Element</u></a>                             | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20100146492</u></a> | <a href="#"><u>Translation of Programming Code</u></a>  | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20100146112</u></a> | <a href="#"><u>Efficient Communication Techniques</u></a>   | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20100146111</u></a> | <a href="#"><u>Efficient Communication in a Network</u></a>   | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20090313613</u></a> | <a href="#"><u>Methods and Apparatus for Automatic Translation of a Computer Program Language Code</u></a>              | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20090313004</u></a> | <a href="#"><u>Platform-Independent Application Development Framework</u></a>   | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20090279562</u></a> | <a href="#"><u>Content-aware dynamic network resource allocation</u></a>  | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20080040630</u></a> | <a href="#"><u>Time-Value Curves to Provide Dynamic QoS for Time Sensitive File</u></a>                                 | <a href="#"><u>Link</u></a> |

Transfers

|                                       |  |                             |
|---------------------------------------|--|-----------------------------|
| <a href="#"><u>US 20070169171</u></a> | <a href="#"><u>Technique for authenticating network users</u></a>  | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20060123481</u></a> | <a href="#"><u>Method and apparatus for network immunization</u></a>   | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20060075042</u></a> | <a href="#"><u>Extensible Resource Messaging Between User Applications and Network Elements in a Communication Network</u></a>   | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20050083960</u></a> | <a href="#"><u>Method and Apparatus for Transporting Parcels of Data Using Network Elements with Network Element Storage</u></a> | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20050076339</u></a> | <a href="#"><u>Method and Apparatus for Automated Negotiation for Resources on a Switched Underlay Network</u></a>               | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20050076336</u></a> | <a href="#"><u>Method and Apparatus for Scheduling Resources on a Switched Underlay Network</u></a>                              | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20050076173</u></a> | <a href="#"><u>Method And Apparatus for Preconditioning Data to Be Transferred on a Switched Underlay Network</u></a>            | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20050076099</u></a> | <a href="#"><u>Method and Apparatus for Live Streaming Media Replication in a Communication Network</u></a>                      | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20050074529</u></a> | <a href="#"><u>Method and apparatus for transporting visualization information on a switched underlay network</u></a>            | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20040076161</u></a> | <a href="#"><u>Dynamic Assignment of Traffic Classes to a Priority Queue in a Packet Forwarding Device</u></a>                   | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20020021701</u></a> | <a href="#"><u>Dynamic Assignment of Traffic Classes to a Priority Queue in a Packet Forwarding Device</u></a>                   | <a href="#"><u>Link</u></a> |
| <a href="#"><u>WO 2006/063052</u></a> | <a href="#"><u>Method and apparatus for network immunization</u></a>   | <a href="#"><u>Link</u></a> |
| <a href="#"><u>WO 2007/008976</u></a> | <a href="#"><u>Technique for authenticating network users</u></a>  | <a href="#"><u>Link</u></a> |
| <a href="#"><u>WO2000/0054460</u></a> | <a href="#"><u>Method and apparatus for accessing network information on a network device</u></a>                                | <a href="#"><u>Link</u></a> |
| <a href="#"><u>WO/2016/203460</u></a> | <a href="#"><u>Ultra-low phase noise frequency synthesizer</u></a>   | <a href="#"><u>Link</u></a> |
| <a href="#"><u>WO/2005/033899</u></a> | <a href="#"><u>Method and apparatus for scheduling resources on a switched underlay network</u></a>                              | <a href="#"><u>Link</u></a> |
| <a href="#"><u>WO/2000/041368</u></a> | <a href="#"><u>Dynamic assignment of traffic classes to a priority queue in a packet forwarding device</u></a>                   | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20140156556</u></a> | <a href="#"><u>Time-variant rating system and method thereof</u></a>   | <a href="#"><u>Link</u></a> |

|                                       |   |                             |
|---------------------------------------|---|-----------------------------|
| <a href="#"><u>US 20140156758</u></a> | <a href="#"><u>Reliable rating system and method thereof</u></a>  | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20170085708</u></a> | <a href="#"><u>Systems and methods for visual presentation and selection of ivr menu</u></a>                                  | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20160373117</u></a> | <a href="#"><u>Ultra-low phase noise frequency synthesizer</u></a>  | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20170322687</u></a> | <a href="#"><u>Systems and methods for electronic communications</u></a>  | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20170302282</u></a> | <a href="#"><u>Radar target detection system for autonomous vehicles with ultra-low phase noise frequency synthesizer</u></a> | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20180019755</u></a> | <a href="#"><u>Radar target detection system for autonomous vehicles with ultra-low phase noise frequency synthesizer</u></a> | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20170289332</u></a> | <a href="#"><u>Systems and methods for visual presentation and selection of ivr menu</u></a>                                  | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20170269797</u></a> | <a href="#"><u>Systems and methods for electronic communication</u></a>   | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20170099058</u></a> | <a href="#"><u>Ultra-low phase noise frequency synthesizer</u></a>  | <a href="#"><u>Link</u></a> |
| <a href="#"><u>US 20170099057</u></a> | <a href="#"><u>Ultra-low phase noise frequency synthesizer</u></a>  | <a href="#"><u>Link</u></a> |

## Publications

*(Not an exhaustive list)*

- [Dangerous Liaisons - Software Combinations as Derivative Works?](#) Determann L.; Berkeley Technology Law Journal. Volume 21, Issue 4, Fall 2006.
- “R&D Models for Advanced Development & Corporate Research” Understanding Six Models of Advanced R&D - Ikhlaz Sidhu, Tal Lavian, Victoria Howell - University of California, Berkeley. Accepted paper for 2015 ASEE Annual Conference and Exposition- June 2015
- “Communications Architecture in Support of Grid Computing”, Tal Lavian, Scholar's Press 2013 ISBN 978-3-639-51098-0.
- [“Applications Drive Secure Light-path Creation across Heterogeneous Domains](#), Feature Topic Optical Control Planes for Grid Networks: Opportunities, Challenges and the Vision.” Gommans L.; Van Oudenaarde B.; Dijkstra F.; De Laat C.; Lavian T.; Monga I.; Taal A.; Travostino F.; Wan A.; IEEE Communications Magazine, vol. 44, no. 3, March 2006, pp. 100-106.
- [Lambda Data Grid: Communications Architecture in Support of Grid Computing](#). Tal I. Lavian, Randy H. Katz; Doctoral Thesis, University of California at Berkeley. January 2006.
- “Information Switching Networks.” Hoang D.B.; T. Lavian; The 4th Workshop on the Internet, Telecommunications and Signal Processing, WITSP2005, December 19-21, 2005, Sunshine Coast, Australia.
- [“Impact of Grid Computing on Network Operators and HW Vendors.”](#) Allcock B.; Arnaud B.; Lavian T.; Papadopoulos P.B.; Hasan M.Z.; Kaplow W.; *IEEE Hot Interconnects at Stanford University 2005*, pp.89-90.
- [DWDM-RAM: A Data Intensive Grid Service Architecture Enabled by Dynamic Optical Networks](#). Lavian T.; Mambretti J.; Cutrell D.; Cohen H.J.; Merrill S.; Durairaj R.; Daspit P.; Monga I.; Naiksatam S.; Figueira S.; Gutierrez D.; Hoang D.B., Travostino F.; *CCGRID 2004*, pp. 762-764.
- [DWDM-RAM: An Architecture for Data Intensive Service Enabled by Next Generation Dynamic Optical Networks](#). Hoang D.B.; Cohen H.; Cutrell D.; Figueira S.; Lavian T.; Mambretti J.; Monga I.; Naiksatam S.; Travostino F.; *Proceedings IEEE Globecom 2004, Workshop on High-Performance Global Grid Networks*, Houston, 29 Nov. to 3 Dec. 2004, pp.400-409.
- [Implementation of a Quality of Service Feedback Control Loop on Programmable Routers](#). Nguyen C.; Hoang D.B.; Zhao, I.L.; Lavian, T.; *Proceedings, 12th IEEE International Conference on Networks 2004. (ICON 2004) Singapore, Volume 2, 16-19 Nov. 2004*, pp.578-582.
- [A Platform for Large-Scale Grid Data Service on Dynamic High-Performance Networks](#). Lavian T.; Hoang D.B.; Mambretti J.; Figueira S.; Naiksatam S.; Kaushil N.; Monga I.; Durairaj R.; Cutrell D.; Merrill S.; Cohen H.; Daspit P.; Travostino F.; *GridNets 2004, San Jose, CA., October 2004*.
- [DWDM-RAM: Enabling Grid Services with Dynamic Optical Networks](#). Figueira S.; Naiksatam S.; Cohen H.; Cutrell D.; Daspit, P.; Gutierrez D.; Hoang D. B.; Lavian T.; Mambretti J.; Merrill S.; Travostino F.; *Proceedings, 4th IEEE/ACM International Symposium on Cluster Computing and the Grid, Chicago, USA, April 2004*, pp. 707-714.
- [DWDM-RAM: Enabling Grid Services with Dynamic Optical Networks](#). Figueira S.; Naiksatam S.; Cohen H.; Cutrell D.; Gutierrez D.; Hoang D.B.; Lavian T.; Mambretti J.; Merrill S.;

Travostino F.; 4th IEEE/ACM International Symposium on Cluster Computing and the Grid, Chicago, USA, April 2004.

- [An Extensible, Programmable, Commercial-Grade Platform for Internet Service Architecture.](#) Lavian T.; Hoang D.B.; Travostino F.; Wang P.Y.; Subramanian S.; Monga I.; IEEE Transactions on Systems, Man, and Cybernetics on Technologies Promoting Computational Intelligence, Openness and Programmability in Networks and Internet Services Volume 34, Issue 1, Feb. 2004, pp.58-68.
- [DWDM-RAM: An Architecture for Data Intensive Service Enabled by Next Generation Dynamic Optical Networks.](#) Lavian T.; Cutrell D.; Mambretti J.; Weinberger J.; Gutierrez D.; Naiksatam S.; Figueira S.; Hoang D. B.; Supercomputing Conference, SC2003 Igniting Innovation, Phoenix, November 2003.
- [Edge Device Multi-Unicasting for Video Streaming.](#) Lavian T.; Wang P.; Durairaj R.; Hoang D.; Travostino F.; Telecommunications, 2003. ICT 2003. 10th International Conference on Telecommunications, Tahiti, Volume 2, 23 Feb.-1 March, 2003 pp. 1441-1447.
- [The SAHARA Model for Service Composition Across Multiple Providers.](#) Raman B.; Agarwal S.; Chen Y.; Caesar M.; Cui W.; Lai K.; Lavian T.; Machiraju S.; Mao Z. M.; Porter G.; Roscoe T.; Subramanian L.; Suzuki T.; Zhuang S.; Joseph A. D.; Katz Y.H.; Stoica I.; Proceedings of the First International Conference on Pervasive Computing. ACM Pervasive 2002, pp. 1-14.
- [Enabling Active Flow Manipulation in Silicon-Based Network Forwarding Engines.](#) Lavian T.; Wang P.; Travostino F.; Subramanian S.; Duraraj R.; Hoang D.B.; Sethaput V.; Culler D.; Proceeding of the Active Networks Conference and Exposition, 2002.(DANCE) 29-30 May 2002, pp. 65-76.
- [Practical Active Network Services within Content-Aware Gateways.](#) Subramanian S.; Wang P.; Durairaj R.; Rasimas J.; Travostino F.; Lavian T.; Hoang D.B.; Proceeding of the DARPA Active Networks Conference and Exposition, 2002.(DANCE) 29-30 May 2002, pp. 344-354.
- [Active Networking on a Programmable Network Platform.](#) Wang P.Y.; Lavian T.; Duncan R.; Jaeger R.; Fourth IEEE Conference on Open Architectures and Network Programming (OPENARCH), Anchorage, April 2002.
- [Intelligent Network Services through Active Flow Manipulation.](#) Lavian T.; Wang P.; Travostino F.; Subramanian S.; Hoang D.B.; Sethaput V.; IEEE Intelligent Networks 2001 Workshop (IN2001), Boston, May 2001.
- [Intelligent Network Services through Active Flow Manipulation.](#) Lavian T.; Wang P.; Travostino F.; Subramanian S.; Hoang D.B.; Sethaput V.; Intelligent Network Workshop, 2001 IEEE 6-9 May 2001, pp.73 -82.
- [Enabling Active Flow Manipulation in Silicon-based Network Forwarding Engine.](#) Lavian, T.; Wang, P.; Travostino, F.; Subramanian S.; Hoang D.B.; Sethaput V.; Culler D.; Journal of Communications and Networks, March 2001, pp.78-87.
- [Active Networking on a Programmable Networking Platform.](#) Lavian T.; Wang P.Y.; IEEE Open Architectures and Network Programming, 2001, pp. 95-103.
- [Enabling Active Networks Services on a Gigabit Routing Switch.](#) Wang P.; Jaeger R.; Duncan R.; Lavian T.; Travostino F.; 2nd Workshop on Active Middleware Services, 2000.
- [Dynamic Classification in Silicon-Based Forwarding Engine Environments.](#) Jaeger R.; Duncan R.; Travostino F.; Lavian T.; Hollingsworth J.; Selected Papers. 10th IEEE Workshop on Metropolitan Area and Local Networks, 1999. 21-24 Nov. 1999, pp.103-109.
- [Open Programmable Architecture for Java-Enabled Network Devices.](#) Lavian, T.; Jaeger, R. F.; Hollingsworth, J. K.; IEEE Hot Interconnects Stanford University, August 1999, pp. 265-277.

- *Open Java SNMP MIB API*. Rob Duncan, Tal Lavian, Roy Lee, Jason Zhou, Bay Architecture Lab Technical Report TR98-038, December 1998.
- *Java-Based Open Service Interface Architecture*. Lavian T.; Lau S.; BAL TR98-010 Bay Architecture Lab Technical Report, March 1998.
- *Parallel SIMD Architecture for Color Image Processing*. Lavian T. Tel – Aviv University, Tel – Aviv, Israel, November 1995.
- [\*Grid Network Services. Draft-ggf-ghpn-netservices-1.0\*](#). George Clapp, Tiziana Ferrari, Doan B. Hoang, Gigi Karmous-Edwards, Tal Lavian, Mark J. Leese, Paul Mealor, InderMonga, Volker Sander, Franco Travostino, Global Grid Forum(GGF).
- [\*Project DRAC: Creating an applications-aware network\*](#). Travostino F.; Keates R.; Lavian T.; Monga I.; Schofield B.; Nortel Technical Journal, February 2005, pp. 23-26.
- [\*Optical Network Infrastructure for Grid. Draft-ggf-ghpn-opticalnets-1\*](#). Dimitra Simeonidou, Reza Nejabati, Bill St. Arnaud, Micah Beck, Peter Clarke, Doan B. Hoang, David Hutchison, Gigi Karmous-Edwards, Tal Lavian, Jason Leigh, Joe Mambretti, Volker Sander, John Strand, Franco Travostino, Global Grid Forum(GGF) GHPN Standard GFD-I.036 August 2004.
- [\*Popeye - Using Fine-grained Network Access Control to Support Mobile Users and Protect Intranet Hosts\*](#). Mike Chen, Barbara Hohlt, Tal Lavian, December 2000.
- Open Networking - Better Networking through Programmability, Open Networking - Better Networking through Programmability

## Presentations and Talks

(Not an exhaustive list)

- [Lambda Data Grid](#)
- [A Platform for Large-Scale Grid Data Service on Dynamic High-Performance Networks](#)
- [Lambda Data Grid: An Agile Optical Platform for Grid Computing and Data-intensive Applications](#).
- [Workflow Integrated Network Resource Orchestration](#)
- [DWDM-RAM: DARPA-Sponsored Research for Data Intensive Service-on-Demand Advanced Optical Networks](#)
- [Impact of Grid Computing on Network Operators and HW Vendors](#)
- [Web Services and OGSA](#)
- [WINER Workflow Integrated Network Resource Orchestration](#).
- [A Grid Proxy Architecture for Network Resources](#)
- [Technology & Society](#)
- [Abundant Bandwidth and how it affects us?](#)
- [Active Content Networking \(ACN\)](#)
- [DWDM-RAM: Enabling Grid Services with Dynamic Optical Networks](#)
- [Application-engaged Dynamic Orchestration of Optical Network Resources](#)
- [DWDM-RAM: DARPA-Sponsored Research for Data Intensive Service-on-Demand Advanced Optical Networks](#)
- [An Architecture for Data Intensive Service Enabled by Next Generation Optical Networks](#)
- [A Platform for Data Intensive Services Enabled by Next Generation Dynamic Optical Networks](#)
- [A Platform for Data Intensive Services Enabled by Next Generation Dynamic Optical Networks](#)
- [Optical Networks](#)
- [Grid Optical Network Service Architecture for Data Intensive Applications](#)
- [Optical Networking & DWDM](#)



- [OptiCal Inc.](#)
- [OptiCal & LUMOS Networks](#)
- [Optical Networking Services](#)
- [Optical Networks](#)
- [Business Models for Dynamically Provisioned Optical Networks](#)
- [Business Model Concepts for Dynamically Provisioned Optical Networks](#)
- [Optical Networks Infrastructure](#)
- [Research Challenges in agile optical networks](#)
- [Services and Applications' infrastructure for agile optical networks](#)
- [Impact on Society](#)
- [Technology & Society](#)
- [TeraGrid Communication and Computation](#)
- [Unified Device Management via Java-enabled Network Devices](#)
- [Active Network Node in Silicon-Based L3 Gigabit Routing Switch](#)
- [Enabling Active Flow Manipulation \(AFM\) in Silicon-based Network Forwarding Engines](#)
- [Enabling Active Flow Manipulation \(AFM\) in Silicon-based Network Forwarding Engines](#)
- [Active Nets Technology Transfer through High-Performance Network Devices](#)
- [Enabling Active Networks Services on A Gigabit Routing Switch](#)
- [Programmable Network Node: Applications](#)
- [Open Innovation via Java-enabled Network Devices](#)
- [Practical Considerations for Deploying a Java Active Networking Platform](#)
- [Open Programmable Architecture for Java-enabled Network Devices](#)
- [Enabling Active Flow Manipulation In Silicon-based Network Forwarding Engines](#)
- [Enabling Active Flow Manipulation In Silicon-based Network Forwarding Engines](#)
- [Enabling Active Flow Manipulation In Silicon-based Network Forwarding Engines](#)
- [DWDM-RAM: DARPA-Sponsored Research for Data Intensive Service-on-Demand Advanced Optical Networks](#)
- [DWDM-RAM: DARPA-Sponsored Research for Data Intensive Service-on-Demand Advanced Optical Networks](#)
- [Open Programmable Architecture for Java-enabled Network Devices](#)
- [Open Java-Based Intelligent Agent Architecture for Adaptive Networking Devices](#)
- [Edge Device Multi-unicasting for Video Streaming](#)
- [Intelligent Network Services through Active Flow Manipulation](#)
- [Java SNMP Oplet](#)
- [Unified Device Management via Java-enabled Network Devices](#)
- [Dynamic Classification in a Silicon-Based Forwarding Engine](#)
- [Integrating Active Networking and Commercial-Grade Routing Platforms](#)
- [Enabling Active Flow Manipulation In Silicon-based Network Forwarding Engines](#)
- [Open Distributed Networking Intelligence: A New Java Paradigm](#)
- [Open Networking Better Networking Through Programmability](#)
- [Open Networking](#)
- [Open Programmability](#)
- [Active Networking On A Programmable Networking Platform](#)
- [Open Networking through Programmability](#)
- [Open Programmable Architecture for Java-enabled Network Devices](#)
- [Popeye – Fine-grained Network Access Control for Mobile Users](#)

- [Integrating Active Networking and Commercial-Grade Routing Platforms](#)
- [Active Networking](#)
- [Programmable Network Devices](#)
- [Open Programmable Architecture for Java-enabled Network Devices](#)
- [To be smart or not to be?](#)



# **EXHIBIT 2**

(12) **United States Patent**  
**Signaoff et al.**

(10) **Patent No.:** **US 7,710,978 B2**  
(45) **Date of Patent:** **May 4, 2010**

(54) **SYSTEM AND METHOD FOR TRAVERSING A FIREWALL WITH MULTIMEDIA COMMUNICATION**

(75) Inventors: **Christopher S. Signaoff**, Hutto, TX (US); **Tom W. Opsahl**, Flower Mound, TX (US); **Edward M. Riley, III**, Flower Mound, TX (US); **Justin S. Signaoff**, Round Rock, TX (US)

(73) Assignee: **directPacket Research, Inc.**, Irving, TX (US)

(\*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 398 days.

|                |         |                  |         |
|----------------|---------|------------------|---------|
| 6,614,465 B2   | 9/2003  | Alexander et al. |         |
| 6,633,324 B2   | 10/2003 | Stephens, Jr.    |         |
| 6,633,985 B2 * | 10/2003 | Drell            | 726/11  |
| 6,735,626 B1   | 5/2004  | Tezuka et al.    |         |
| 6,795,444 B1   | 9/2004  | Vo et al.        |         |
| 6,798,782 B1   | 9/2004  | Caronni et al.   |         |
| 6,963,583 B1   | 11/2005 | Foti et al.      |         |
| 7,016,935 B2   | 3/2006  | Lee et al.       |         |
| 7,020,130 B2 * | 3/2006  | Krause et al.    | 370/352 |
| 7,023,465 B2   | 4/2006  | Stephens, Jr.    |         |
| 7,031,341 B2 * | 4/2006  | Yu               | 370/469 |
| 7,039,701 B2   | 5/2006  | Wesley           |         |

(21) Appl. No.: **11/403,549**

(Continued)

(22) Filed: **Apr. 13, 2006**

**OTHER PUBLICATIONS**

(65) **Prior Publication Data**  
US 2007/0242696 A1 Oct. 18, 2007

International Search Report and Written Opinion issued for PCT/US2007/066435; Dated: Apr. 2, 2008; 9 Pages.

(Continued)

(51) **Int. Cl.**  
**H04L 12/28** (2006.01)  
**H04L 12/66** (2006.01)  
**H04L 29/06** (2006.01)  
**H04J 3/16** (2006.01)  
**H04K 1/00** (2006.01)

*Primary Examiner*—Alpus H Hsu  
(74) *Attorney, Agent, or Firm*—Fulbright & Jaworski L.L.P.

(57) **ABSTRACT**

(52) **U.S. Cl.** ..... **370/395.5; 370/401; 370/466; 370/469; 380/255; 713/151; 726/3**

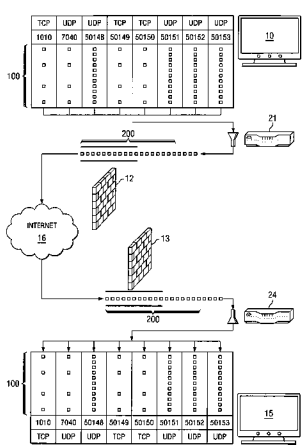
(58) **Field of Classification Search** ..... **370/395.5; 370/401, 466, 469; 380/255; 713/151; 726/3**  
See application file for complete search history.

Systems and methods are disclosed for transporting multiport protocol traffic using a single-port protocol. Multiport protocol traffic from a first endpoint is converted into a single-port protocol for transport across a network. The traffic is sent over a commonly-open port and received at a second endpoint before being dispersed to the appropriate ports of the second endpoint. By converting the traffic to a single-port protocol and choosing which commonly open port to communicate the traffic through, firewalls between each endpoint may be traversed without changing any of their settings.

(56) **References Cited**  
**U.S. PATENT DOCUMENTS**

|              |        |                   |
|--------------|--------|-------------------|
| 6,047,320 A  | 4/2000 | Tezuka et al.     |
| 6,266,809 B1 | 7/2001 | Craig et al.      |
| 6,380,968 B1 | 4/2002 | Alexander et al.  |
| 6,434,140 B1 | 8/2002 | Barany et al.     |
| 6,611,503 B1 | 8/2003 | Fitzgerald et al. |

**30 Claims, 5 Drawing Sheets**



## US 7,710,978 B2

Page 2

## U.S. PATENT DOCUMENTS

|              |      |         |                                |              |      |         |                              |
|--------------|------|---------|--------------------------------|--------------|------|---------|------------------------------|
| 7,159,036    | B2   | 1/2007  | Hinchliffe et al.              | 2005/0243747 | A1   | 11/2005 | Rudolph                      |
| 7,177,929    | B2   | 2/2007  | Burbeck et al.                 | 2005/0259145 | A1   | 11/2005 | Schrader et al.              |
| 7,181,530    | B1   | 2/2007  | Halasz et al.                  | 2005/0271051 | A1   | 12/2005 | Holloway et al.              |
| 7,194,526    | B2   | 3/2007  | Kanemitsu                      | 2006/0098684 | A1   | 5/2006  | Bozzonek et al.              |
| 7,206,808    | B2   | 4/2007  | Babka et al.                   | 2006/0104288 | A1 * | 5/2006  | Yim et al. .... 370/395.52   |
| 7,251,689    | B2   | 7/2007  | Wesley                         | 2006/0109862 | A1   | 5/2006  | Choi et al.                  |
| 7,293,169    | B1   | 11/2007 | Righi et al.                   | 2006/0187903 | A1   | 8/2006  | Kallio et al.                |
| 7,328,406    | B2   | 2/2008  | Kalinoski et al.               | 2006/0190719 | A1 * | 8/2006  | Rao et al. .... 713/160      |
| 7,346,076    | B1   | 3/2008  | Habiby et al.                  | 2006/0224883 | A1 * | 10/2006 | Khosravi et al. .... 713/151 |
| 7,346,912    | B2   | 3/2008  | Seebaldt                       | 2007/0005804 | A1 * | 1/2007  | Rideout .... 709/246         |
| 7,353,380    | B2 * | 4/2008  | VanHeyningen .... 713/150      | 2007/0022201 | A1   | 1/2007  | Aaby et al.                  |
| 7,363,381    | B2   | 4/2008  | Mussman et al.                 | 2007/0036143 | A1   | 2/2007  | Alt et al.                   |
| 7,370,097    | B2   | 5/2008  | Hashimoto                      | 2007/0239841 | A1   | 10/2007 | Lehrman                      |
| 7,372,957    | B2   | 5/2008  | Strathmeyer et al.             | 2007/0242696 | A1   | 10/2007 | Signaoff et al.              |
| 7,385,622    | B2   | 6/2008  | Babka et al.                   | 2008/0043091 | A1   | 2/2008  | Lia et al.                   |
| 7,436,428    | B2   | 10/2008 | Schrader et al.                | 2008/0134200 | A1   | 6/2008  | Seebaldt                     |
| 7,441,270    | B1 * | 10/2008 | Edwards et al. .... 726/15     | 2008/0235362 | A1   | 9/2008  | Kjesbu et al.                |
| 2003/0065737 | A1   | 4/2003  | Aasman                         | 2009/0051752 | A1   | 2/2009  | Lammers                      |
| 2003/0081783 | A1 * | 5/2003  | Adusumilli et al. .... 380/270 | 2009/0112671 | A1   | 4/2009  | Grodum                       |
| 2003/0182451 | A1   | 9/2003  | Grass et al.                   |              |      |         |                              |
| 2003/0227908 | A1   | 12/2003 | Scoggins et al.                |              |      |         |                              |
| 2003/0232648 | A1 * | 12/2003 | Prindle .... 463/40            |              |      |         |                              |
| 2004/0037268 | A1   | 2/2004  | Read                           |              |      |         |                              |
| 2004/0158606 | A1   | 8/2004  | Tsai                           |              |      |         |                              |
| 2005/0021610 | A1   | 1/2005  | Bozzonek et al.                |              |      |         |                              |
| 2005/0122964 | A1   | 6/2005  | Strathmeyer et al.             |              |      |         |                              |
| 2005/0125696 | A1   | 6/2005  | Afshar et al.                  |              |      |         |                              |

## OTHER PUBLICATIONS

International Search Report and Written Opinion issued for PCT/US2007/066451; Dated: Jul. 7, 2008; 11 Pages.  
 International Search Report and Written Opinion issued for PCT/US07/66457 dated Jun. 17, 2008, 10 pgs.  
 International Search Report and Written Opinion issued for PCT/US2007/066460; Dated: Apr. 9, 2008; 10 Pages.

\* cited by examiner



FIG. 2

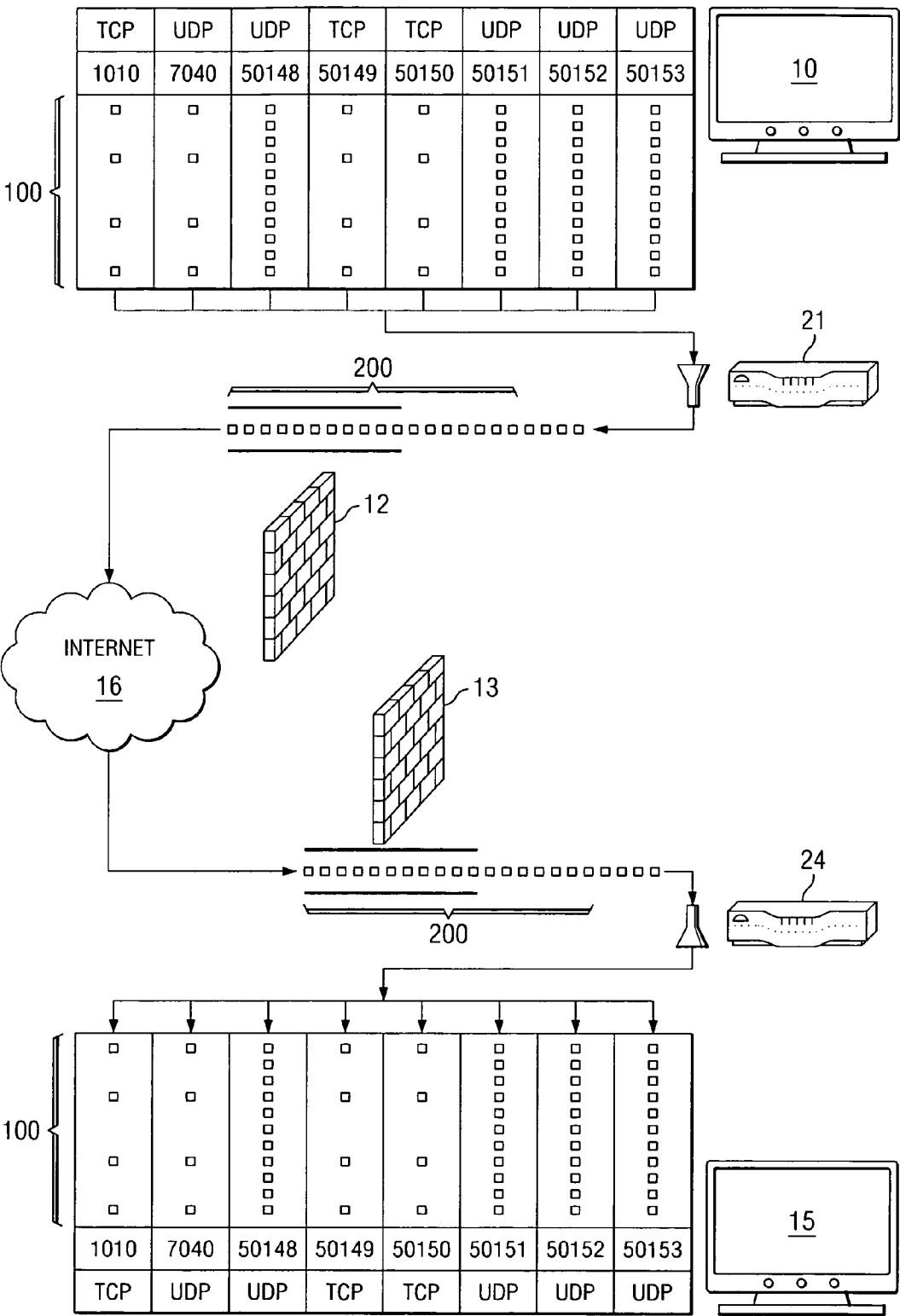


FIG. 3

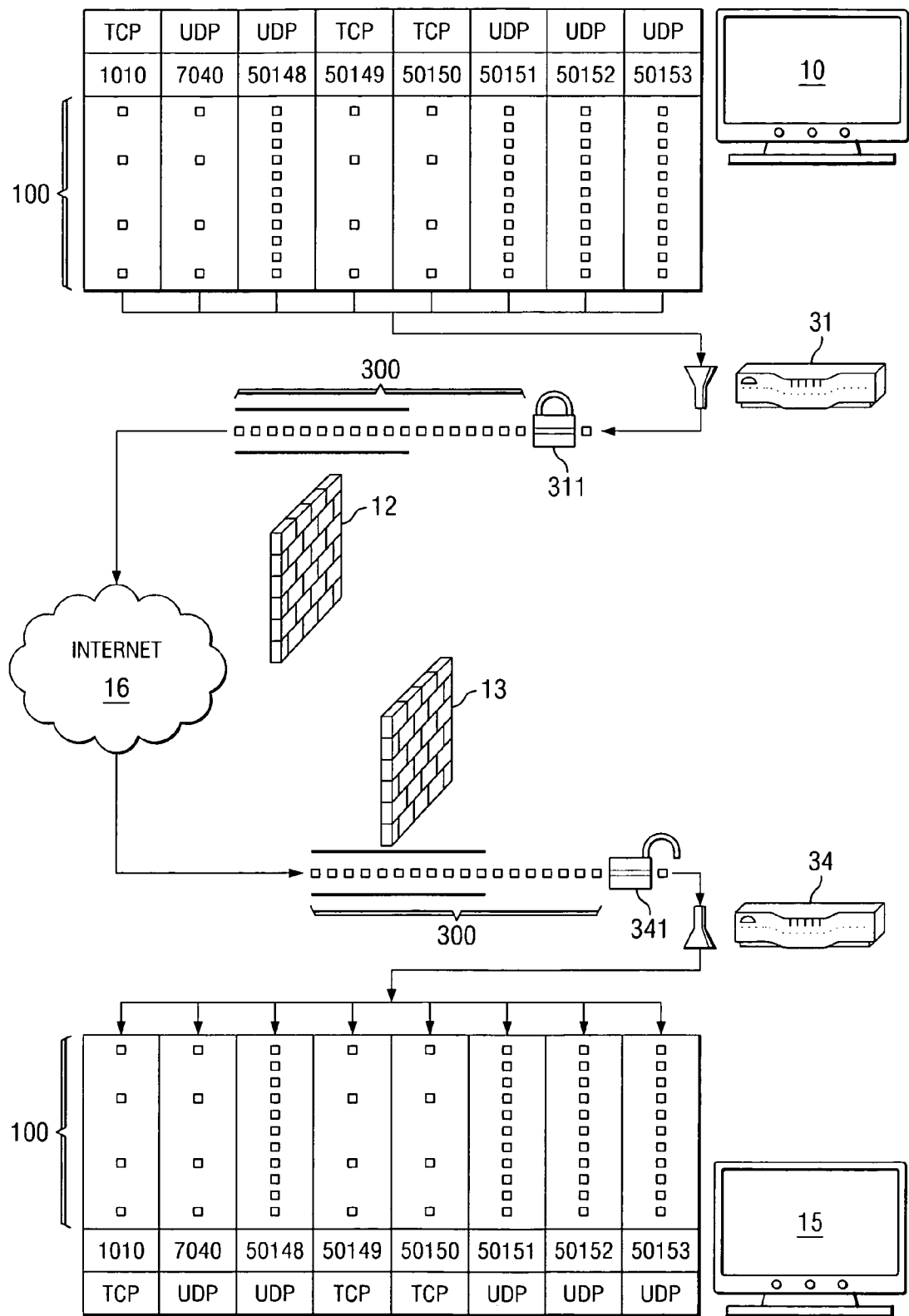
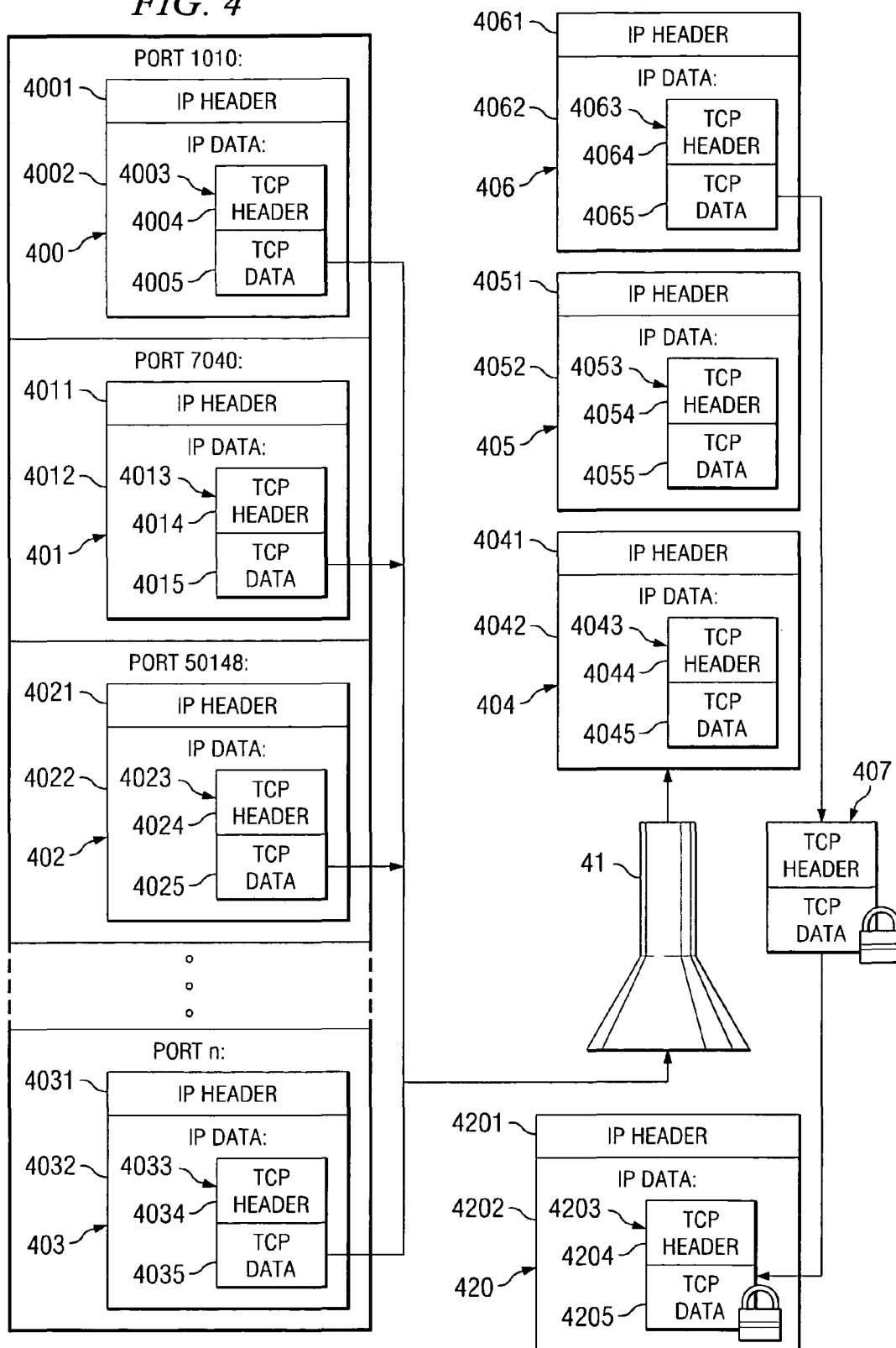
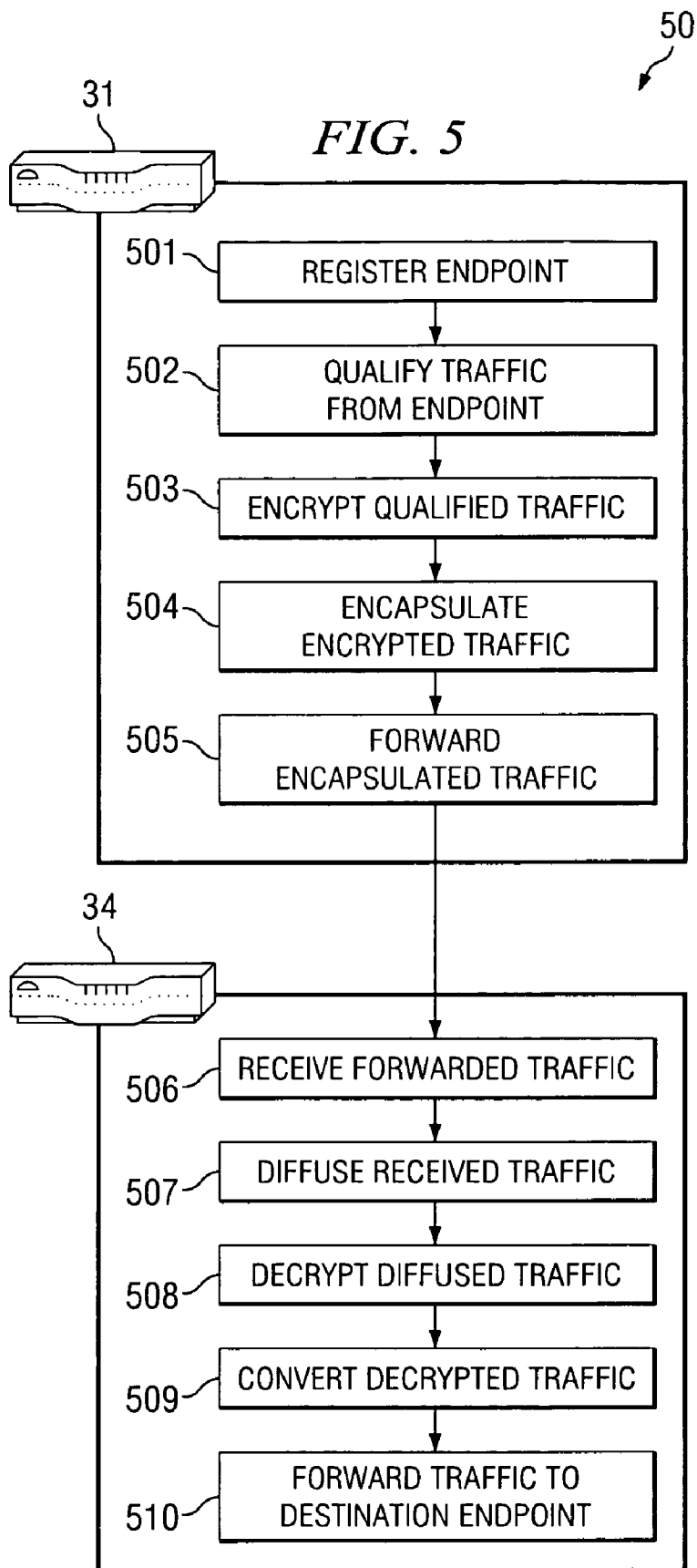


FIG. 4







US 7,710,978 B2

1

# SYSTEM AND METHOD FOR TRAVERSING A FIREWALL WITH MULTIMEDIA COMMUNICATION

## TECHNICAL FIELD

The present invention relates, in general, to electronic communications, and, more specifically, to transmitting communication data within a multimedia communication system.

## BACKGROUND OF THE INVENTION

The Internet may be used for many forms of communication, including voice conversations, video conferencing, development collaboration, and the like. In order for a manufacturers' programs, applications, equipment, and systems to be interoperable with each other, many protocols have been developed to standardize the communication between such systems. These protocols have grown increasingly complex to handle all the types of traffic generated to facilitate communication for video conferencing, voice over Internet Protocol (VoIP), and data over Internet Protocol applications. Two such protocols are H.323 from the International Telecommunication Union—Telecommunication Standardization Sector (ITU-T) and the Session Initiation Protocol (SIP) from the Internet Engineering Task Force (IETF). Both H.323 and SIP typically allow for multimedia communication including voice, video, and data communications in real-time.

In Internet Protocol (IP) communication networks, devices or endpoints on the network are identified by their respective IP address. Applications and programs on the different devices further identify each other using port numbers. A port number is a sixteen bit integer, the value of which falls into one of three ranges: the well-known ports, ranging from 0 through 1023; the registered ports, ranging from 1024 through 49151; and the dynamic and/or private ports, ranging from 49152 through 65535. The well-known ports are reserved for assignment by the Internet Corporation for Assigned Names and Numbers (ICANN) for use by applications that communicate using the Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) and generally can only be used by a system/root process or by a program run by a privileged user. The registered ports may be registered for use by companies or other individuals for use by applications that communicate using TCP or UDP. The dynamic or private ports, by definition, cannot be officially registered nor are they assigned. Both the H.323 and SIP standards use multiple, well-known, registered, and/or dynamic ports in order to facilitate such communication.

H.323 and SIP each rely on multiple other protocols, some of which may in turn rely on UDP for sending and receiving multimedia traffic. UDP features minimal overhead compared to other transport protocols (most notably TCP) at the expense of having less reliability. UDP does not provide for guaranteed packet delivery nor data integrity. UDP does offer the highest possible throughput, thus, making it ideally suited for multimedia real-time communications.

Multimedia communications traffic will most likely have to traverse a firewall at some point during transmission, especially over the Internet, regardless to which protocol the traffic conforms. Firewalls are used in modem networks to screen out unwanted or malicious traffic. One of many techniques a firewall may use is packet filtering, wherein the firewall determines whether or not to allow individual packets by analyzing information in the packet header (such as the IP address and port of the source and destination). Thus, various ports or IP

2

addresses may be blocked to minimize the risk of allowing malicious traffic into an important computer network or system. Another more advanced technique is called stateful inspection, wherein in addition to analyzing header information, a firewall keeps track of the status of any connection opened by network devices behind the firewall. Deciding whether or not a packet is dropped in a stateful inspection is based on the tracked status of the connection and information from within the packet header. In practice, firewalls (especially those used by large corporations) generally only allow traffic from the well-known ports, though such firewalls may be specially configured to allow traffic on any port. For multimedia communication systems that use multiple registered and dynamic ports, firewalls (unless specially configured) will generally block the data traffic on these ports between multimedia systems, thus, preventing communication.

Video conferencing endpoints generally use multiple dynamic ports for the transmission of communication data packets and, as such, each port used necessitates opening that port on a firewall. Additionally, different endpoints participating in different conversations use different sets of ports, further increasing the number of ports to be opened on a firewall. Reconfiguring ports on a firewall is a time consuming task that introduces the risk of human error, which may defeat the purpose of the firewall by leaving a network vulnerable to malicious attacks. Furthermore, even though these dynamic ports should be closed after the communication ends, in practice, once a firewall port is open, it remains open because the firewall technicians typically do not expend the additional time resources to close the ports.

Additionally, many video conferencing systems do not support encryption. In such cases the communication between endpoints is not secure and may be intercepted while being transmitted across the Internet.

Existing video conferencing systems such as TANDBERG's BORDER CONTROLLER™, a component of TANDBERG's EXPRESSWAY™ firewall traversal solution, requires the use of TANDBERG Gatekeepers or TANDBERG traversal enabled endpoints. While allowing firewall traversal, the EXPRESSWAY™ solution still requires user intervention to select and trust a range of ports on a firewall and requires the purchase of TANDBERG equipment to use existing legacy video conference endpoints that are not traversal-enabled. The V2IU™ series of products from Polycom, Inc., are Application Level Gateways (ALG) that act as protocol-aware firewalls that automate the selection and trusting of ports, but as such, multiple ports are still used when sending traffic between endpoints with the risk of having such traffic being blocked by a non-protocol-aware firewall. Further, such an ALG does not provide for secure communication. The PATHFINDER™ series of products from RadVision, Ltd., provides for firewall traversal via multiplexing to a single port, but still requires opening a port on a firewall. Multiplexing is implemented by taking sections of data from each of the data streams coming through the various ports and placing them alternately into a single stream. Thus, the resulting stream is simply a train of interleaved data bits that are not recognized as any particular communication protocol. At the destination end point, a packet constructor picks each data bit and places it in the appropriate stream on the appropriate port and rebuilds the original stream.

Similar systems have been implemented for voice, VoIP, and data over IP communication systems. Each either relies on a proprietary system or equipment or relies on actually selecting and opening multiple ports in a firewall that could leave the underlying network vulnerable to malicious electronic attacks.

## US 7,710,978 B2

3

## BRIEF SUMMARY OF THE INVENTION

The present invention is directed to a system and method for transporting multiport protocol traffic using a single-port protocol that is known to be transmitted on a port that is typically open on standard firewalls. Multiport protocol traffic from a first endpoint is converted in to a single-port protocol for transport across a network. The traffic is then reconverted to the multiport protocol and directed to the appropriate ports at a targeted second endpoint. In being converted into the single-port protocol, the traffic may then traverse a firewall by using a well-known port, such that little or no reconfiguration of the firewall is required. In so doing, the risk of human error leaving a network vulnerable to malicious attacks is reduced. Moreover, instead of creating an unrecognizable data stream, which may still be rejected by more-advanced firewalls, such as through multiplexing, the various embodiments of the present invention actually creates a known, single-port communication protocol.

The foregoing has outlined rather broadly the features and technical advantages of the present invention in order that the detailed description of the invention that follows may be better understood. Additional features and advantages of the invention will be described hereinafter which form the subject of the claims of the invention. It should be appreciated by those skilled in the art that the conception and specific embodiment disclosed may be readily utilized as a basis for modifying or designing other structures for carrying out the same purposes of the present invention. It should also be realized by those skilled in the art that such equivalent constructions do not depart from the spirit and scope of the invention as set forth in the appended claims. The novel features which are believed to be characteristic of the invention, both as to its organization and method of operation, together with further objects and advantages will be better understood from the following description when considered in connection with the accompanying figures. It is to be expressly understood, however, that each of the figures is provided for the purpose of illustration and description only and is not intended as a definition of the limits of the present invention.

## BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present invention, reference is now made to the following descriptions taken in conjunction with the accompanying drawing, in which:

FIG. 1 is a diagram illustrating the flow of packets in a typical IP communication system;

FIG. 2 is a diagram illustrating an IP communication system configured according to one embodiment of the present invention;

FIG. 3 is a diagram illustrating an IP communication system configured according to another embodiment of the present invention, which includes encryption;

FIG. 4 is a diagram illustrating the handling of packets; and

FIG. 5 is a flowchart showing for an embodiment of the invention, example steps that may be employed to traverse a firewall.

## DETAILED DESCRIPTION OF THE INVENTION

A variety of protocols require the use of multiport traffic. Whether the traffic is data between applications, voice communications, or video conferencing, whenever multiport traffic is used there is a possibility of some or all of the traffic

4

being blocked by a firewall between two devices that are attempting to communicate. As an example, video conferencing systems, whether they are based on H.323, SIP, or other similar multimedia communication protocols, use multiple ports and multiple protocols in order to enable two-way audio and video communication. The communication protocols specify different types of traffic that may be sent between endpoints which include media traffic (voice, video, and the like) along with the control traffic (camera, connection control, and the like). The media traffic is comprised of data for the images and sound being transmitted between endpoints with the control traffic comprising data used to control the connection between endpoints and the features of the endpoint (e.g., camera direction, zoom, and the like). Due to its higher throughput rate, UDP may typically be utilized for the real-time communication traffic between endpoints. TCP may be utilized for traffic requiring data integrity (e.g., control traffic). As such, video conferencing systems typically make use of both TCP and UDP to transport the multimedia data to enable communication. The ports that are typically used to enable the two-way communication include various ports across the well-known ports, the registered ports, and the dynamic ports. Firewalls are usually set up to block unrequested traffic and/or traffic coming in on dynamic ports. Furthermore, UDP does not provide a mechanism for identifying received traffic as requested traffic. Thus, programs and endpoints that send traffic conforming to UDP are at risk of having that traffic blocked by the remote endpoint's firewall for both being unrequested and being sent on a blocked port.

Referring to FIG. 1, video conference endpoint 10 attempts to send multimedia data to video conference endpoint 15. Multiprot packets 100 sent from well-known port 1010, registered port 7030, and dynamic ports 50148-50153 are being transmitted to video conference endpoint 15. Firewall 12 passes all the outgoing traffic (packets 100) on all ports since this traffic has originated from the network inside of firewall 12. The traffic is transmitted across Internet 16 and is received by firewall 13, which is operating in a standard mode. In the standard mode, firewall 13 blocks dynamic ports and unrequested traffic (packets 101), such that only the TCP traffic (packets 102) on well-known port 1010 is received by endpoint 15. Thus, with each endpoint being behind their respective firewalls, neither two-way nor one-way communication can take place.

Referring to FIG. 2, video conference endpoint 10 again attempts to send multimedia data (packets 100) to video conference endpoint 15, this time with network devices 21 and 24 in the system. In this embodiment, endpoint 10 is a video conference endpoint that uses a multiple port communication protocol in order to establish communication with endpoint 15. For the purposes of this example, endpoint 10 uses ports 1010, 7030, 50148-50153. The data transmitted using ports 1010 and 50149-50150 utilize TCP as the transport protocol while the data transmitted using ports 7030, 50148, and 50151-50153 utilize UDP as the transport protocol. Packets from each of these ports conforming to these various protocols and sub-protocols are received by network device 21. It should be noted that additional or alternative examples of endpoints may use more or fewer ports of different numbers based in part on the applications or protocols used to facilitate multimedia communication.

The received packets are encapsulated to conform to a protocol used by devices 21 and 24 for transmitting data, which may include, but is not limited to: TCP, UDP, Stream Control Transmission Protocol (SCTP), Datagram Congestion Control Protocol (DCCP), Real-time Transport Protocol (RTP), and the like. Device 21 receives packets 100 from

## US 7,710,978 B2

5

endpoint **10** that conform to both TCP and UDP, encapsulates each of multiport packets **100** into single-port packets **200** that conform to a single-port communication protocol used by devices **21** and **24**, and sends packets **200** to device **24**. The method of encapsulation may comprise using some or all of the information (header and data) within each of packets **100** as the data section for encapsulated packets **200**.

The encapsulated packets are sent to device **24** using any of the well-known or registered ports, which are the ports that are typically open in standard firewalls. One such well-known port that could be chosen is port **443**, which is commonly reserved for HTTPS traffic by ICANN and is commonly open by default on most firewalls. While the packets may be sent along any of the well-known, registered, or dynamic ports, the preferable port used may be a port that is commonly open on most firewalls in their standard configurations (e.g., the well-known ports, certain registered ports, and the like).

Firewall **12** inspects the traffic from device **21** before sending it out through Internet **16** to device **24**. When the traffic arrives at firewall **13**, it inspects the traffic, determines that it is valid traffic on a well-known port, and passes it along to device **24**.

Device **24** receives encapsulated single-port packets **200** sent from device **21**. Device **24** then reconstructs multiport packets **100** using packets **200**. Reconstruction may be performed by any suitable method including hash-like functions or tables. As an example, header information within one of packets **200** may be an input to a hash-like function that returns the destination IP address and port numbers for a given packet. In the case of a hash-like table, device **21** may use a portion of the header or data in each of packets **100** as the index of a hash-like table and then convert packets **100** to packets **200**. Device **24** upon receiving packets **200**, may use a portion of the header or data in each of packets **200** as the index of a hash-like table and then reconvert packets **200** back to packets **100**, recovering the original IP addresses and ports based on information stored in the hash-like table.

From the original headers, device **24** determines for each packet that it is for delivery to endpoint **15**. Device **24** then sends the packets to endpoint **15** using each packet's destination port. Thus, if a port and protocol are advantageously chosen (such as port **443** and Secure Sockets Layer (SSL)), communications traffic from endpoint **10** may be sent to endpoint **15** with no modification or user intervention to traverse firewalls **12** and **13**. While one-way communication is described (from endpoint **10** to endpoint **15**) it is noted that each of devices **21** and **24** may perform the steps of receiving multiple packets, encapsulation, port translation, decapsulation, and resending multiple packets in order to enable two-way communication between endpoints **10** and **15**. Additional or alternative embodiments may use any of the well-known or registered ports that are typically or commonly open in standard firewalls to send packets between devices **21** and **24**. While any of the well-known, registered, or dynamic ports may be used, it is preferable to select a port that is commonly open in firewalls.

It should be noted that in additional or alternative embodiments of the present invention, network or other errors may occasionally lead to lost or corrupted packets and some protocols (such as TCP) specify that in such cases these lost or corrupted packets be resent, which is at odds with maintaining real-time communication. With real-time communication, current data takes precedence over lost previous data since resent packets of previously lost or corrupt data may arrive too late to be useful. As such, when receiving a request to resend a packet containing real-time data (e.g. data corresponding to the audio or video of the communication) devices

6

**21** and **24** may simply ignore the resend request or, alternatively, send a current data packet masquerading as the previously sent and subsequently lost packet, as alternate data.

Referring to FIG. 3, device **31** adds encryption layer **311** to the data. Any method or algorithm of encryption may be used including, but not limited to: 128-bit Advanced Encryption Standard (AES); Triple Data Encryption Standard (TDES); Skipjack, or the like. Some or all of each packet received may be encrypted, including the header, which contains the source and destination port numbers associated with the packet. With all of the packets **100** from endpoint **10** having an added layer of encryption and becoming packets **300**, the media traffic along with the control traffic between endpoints **10** and **15** are secured for transmission across Internet **16**. Device **34** receives secure packets **300** and removes encryption layer **311** before reconstructing packets **100**. The reconstructed packets **100** are then dispersed to endpoint **15** addressed to the appropriate ports expected by endpoint **15**.

In alternative or additional embodiments, devices **21/31** and **24/34** may also qualify their incoming traffic in order to securely pass traffic associated with the connection between endpoints **10** and **15**. As an example, endpoint **10**, upon being connected to device **21/31**, may register itself with device **21/31** as a video conferencing endpoint. When endpoint **10** begins using network ports for a conference call or other connection, device **21/31** may identify those ports as being used and, if appropriate, begin converting and encrypting the traffic associated with such ports. This qualification and registration process may be performed by the use of a hash-like function, so that device **21/31** may efficiently perform the qualification. As an example, endpoint **10** may register port **50152** and start sending packets. For every packet received, the source IP address and port may be the inputs to a hash-like function that determines whether a received packet is qualified for further processing and transmission. In the case of a hash-like table, device **24** may use a portion of the header or data in each of packets **200** as the index of a hash-like table and then determine whether a packet is qualified based on information stored in the hash-like table.

While each of devices **21** and **24** is depicted connected to a single video conferencing system, they may be connected to multiple and various video conference systems, H.323 gatekeepers, H.323 gateways, SIP proxies, SIP registrars, or the like. When multiple video conferencing systems are connected to a device, such as device **21**, any connections or calls that do not require traversing a firewall may accordingly not be converted into a single-port communication protocol. As an example, if two video conference endpoints are on the same network behind a firewall and are engaging in communications, this traffic does not pass through a firewall (the traffic is only transmitted on the internal network). Thus, devices **21/31** may recognize this situation and, accordingly, not encapsulate nor encrypt the traffic between two such endpoints.

Additionally, device **21** need not be a stand-alone device as its functionality may be integrated into any other network device including, but not limited to: video conference systems, firewalls, H.323 gateways, SIP proxies, SIP registrars or the like. Alternative embodiments may also send traffic between endpoints **10** and **15** that conform to any number of standards or protocols for multimedia communication including, but not limited to the H.323 and SIP protocols by converting the multiport communication protocols into a single-port protocol that uses a port that is typically open on most firewalls.

FIG. 4 is a diagram illustrating the handling of packets. Devices implementing the various embodiments of the inven-

## US 7,710,978 B2

7

tion receive multiple IP data packets (400-403) from multiple ports (1010, 7040, 50148, . . . , n). Each packet has an IP header (4001/4011/4021/4031) and an IP data section (4002/4012/4022/4032). The IP header contains information for properly delivering a packet to a destination including, among other things: a source IP address, a destination IP address, and the total length of the packet. The IP data section contains the data being transmitted, which is usually another packet conforming to a different protocol such as TCP, UDP, or the like. The TCP and UDP packets (4003/4013/4023/4033) found within IP packets 400-403, each also have a header (4004/4014/4024/4034) and data (4005/4015/4025/4035) sections. Headers 4004/4014/4024/4034 of TCP and UDP packets 4003/4013/4023/4033 have the source and destination ports of a packet.

Each packet received is treated the same regardless of the packet's source port or to which protocol the packet conforms. After being received, each IP packet's data section (4042/4052/4062) may be encrypted and then become the data section of a new packet, which may conform to a different protocol for single-port communication. As an example, packet 407 is the encrypted TCP packet 4063 of IP packet 406. IP packet 420 contains TCP packet 4203, whose TCP data section 4205 is packet 407. This method allows the original source and destination ports identified in packet 406's TCP header to be saved and also encrypted such that when packet 420 is transmitted across the Internet, it may not be identified as using a port associated with video conferencing, further increasing security. Additionally, in creating a new TCP packet, the port address may effectively be changed. As an example, a packet received from port 1010 could be sent out on port 443, with the original source port being saved in an encrypted form within packet 407. TCP data section 4205 of packet 420 may also contain encrypted or non-encrypted UDP packets, RTP packets, or IP packets instead of the encrypted TCP packet portrayed. As an example, IP packet 406 may be the TCP data 4205 of packet 420. Accordingly, additional or alternative embodiments may encrypt the entire IP packet (404-406) instead of or in addition to the IP data sections (4042/4052/4062).

FIG. 5 is a flowchart that shows for an embodiment of the invention, example steps that may be employed by devices 31 and 34 to traverse a firewall. An endpoint, when connected to a network, first registers with device 31 by the endpoint identifying itself as a compliant endpoint (e.g., it is an endpoint that conforms to H.323, SIP, VoIP, or the like), as shown by step 501.

On a given network, multiple devices may be connected, as such, device 31 may receive traffic from many devices within that network. Thus, device 31 qualifies the traffic it receives to ensure that the traffic sent to device 34 is appropriate traffic. This is shown in step 502 and may be accomplished by comparing a given packet's source IP and port addresses to those of endpoints that have registered with device 31. In step 503, device 31 encrypts the previously qualified traffic securing the communication between two endpoints using any suitable encryption method including, but limited to: AES 128-bit, TDES, Skipjack, or the like. In step 504, the encrypted traffic is then encapsulated to conform to a single port protocol, such as SSL, by placing the previously encrypted packet into a new packet conforming to SSL protocol. As shown by step 505, the encapsulated traffic is then forwarded to device 34.

In step 506, device 34 receives the single port traffic from device 31 and is diffused by step 507 by restoring the original IP addresses and port numbers to the individual packets. In step 508, this diffused traffic is then decrypted, thus, recov-

8

ering the original multimedia and control communication information within the packets. In step 509, the packets are then restored to their original transport protocol, such as TCP, UDP, or the like. With the packets being fully restored, they are then forwarded to the destination endpoint by device 34, as shown by step 510.

It is noted that while the disclosure has used the communication between two video conference endpoints as an example, it is understood that the systems and methods described may be used by other programs, applications, communications systems, and the like, that use multiport protocols for communication. As such, embodiments of the invention may be used for audio systems VoIP systems, or any other system that uses a multiport protocol to transfer data between devices. Referring back to FIG. 2 as an example, endpoints 10 and 15 may be VoIP endpoints engaging in voice communication. In this embodiment the multiport VoIP protocol traffic from endpoint 10 may be received by device 21, converted to a single port protocol by device 21, encapsulated by device 21, transmitted to device 24, decapsulated by device 24, converted back to the original multiport protocol by device 24, transmitted to endpoint 15, and received by endpoint 15, as described in further detail above. The same holds true for other types of programs, equipment, or applications using a multiport protocol to transfer data across a network.

Although the present invention and its advantages have been described in detail, it should be understood that various changes, substitutions and alterations can be made herein without departing from the spirit and scope of the invention as defined by the appended claims. Moreover, the scope of the present application is not intended to be limited to the particular embodiments of the process, machine, manufacture, composition of matter, means, methods and steps described in the specification. As one of ordinary skill in the art will readily appreciate from the disclosure of the present invention, processes, machines, manufacture, compositions of matter, means, methods, or steps, presently existing or later to be developed that perform substantially the same function or achieve substantially the same result as the corresponding embodiments described herein may be utilized according to the present invention. Accordingly, the appended claims are intended to include within their scope such processes, machines, manufacture, compositions of matter, means, methods, or steps.

What is claimed is:

1. A method for communication between two or more endpoints, said method comprising:

receiving, at a first intermediate communication device that is communicatively coupled with a first endpoint communication device, a plurality of multiport packets of data in a multiport communication protocol for communication from the first endpoint communication device;

converting, by said first intermediate communication device, said plurality of multiport packets into a plurality of single-port packets in a single-port communication protocol;

transmitting from said first intermediate communication device said plurality of single-port packets over a commonly-open port to at least a second intermediate communication device that is communicatively coupled with one or more other endpoint communication devices, said plurality of single-port packets traversing one or more firewalls using said commonly-open port;

receiving said plurality of single-port packets at said at least a second intermediate communication device;

## US 7,710,978 B2

9

reconverting, by said at least a second intermediate communication device, said received plurality of single-port packets into said multipoint communication protocol resulting in reconverted plurality of multipoint packets; and

delivering, from said at least a second intermediate communication device to said one or more other endpoint communication devices, said reconverted plurality of multipoint packets using two or more ports associated with said multipoint communication protocol.

2. The method of claim 1, further comprising:

encrypting said plurality of single-port packets in said single-port communication protocol prior to said transmitting.

3. The method of claim 2, further comprising:

decrypting said encrypted plurality of single-port packets prior to said reconverting.

4. The method of claim 2, wherein said encrypting is according to one of:

an Advanced Encryption Standard (AES) 128-bit algorithm;

a Triple Data Encryption Standard (TDES) algorithm; or a Skipjack algorithm.

5. The method of claim 1, wherein:

said single-port communication protocol comprises:

Secure Sockets Layer (SSL) protocol.

6. The method of claim 1, wherein:

a portion of said plurality of multipoint packets conforms to a first transmission protocol of said multipoint communication protocol;

another portion of said plurality of multipoint packets conforms to a second transmission protocol of said multipoint communication protocol; and

wherein said transmitting comprises transmitting said plurality of single-port packets using said first transmission protocol in said single-port communication protocol.

7. The method of claim 6, wherein said first transmission protocol comprises Transmission Control Protocol (TCP); and

said second transmission protocol comprises User Datagram Protocol (UDP).

8. The method of claim 6, further comprising: sending alternate data instead of requested data in response to a resend request.

9. The method of claim 1, further comprising:

qualifying said plurality of multipoint packets, wherein said qualifying comprises:

registering a network device;

using network ports by said registered network device;

determining whether said plurality of multipoint packets originated from a network port used by said registered network device; and

allowing further transmission of said plurality of multipoint packets based on said determining.

10. The method of claim 1, wherein said commonly-open port is a well-known port.

11. The method of claim 1, wherein said commonly-open port is port 443.

12. The method of claim 1 wherein said single-port communication protocol is acceptable by any of a plurality of different commonly-open transmission control protocol (TCP) ports.

13. The method of claim 1 wherein said single-port communication protocol is not hypertext transport protocol (HTTP).

10

14. A system comprising:

a first network device that is communicatively coupled with at least a first endpoint communication device, said first network device comprising:

an interface for receiving a plurality of multipoint packets of data in a multipoint communication protocol from two or more ports for communication from said at least a first endpoint communication device; and

a conversion table for said first network device to convert said plurality of multipoint packets into a plurality of single-port packets in a single-port communication protocol, wherein said single-port communication protocol is acceptable by any of a plurality of different commonly-open transmission control protocol (TCP) ports, and wherein said interface communicates said converted plurality of single-port packets over a selected one of the plurality of different commonly-open TCP ports; and

a second network device that is communicatively coupled with at least a second endpoint communication device, said second network device comprising:

a second interface for receiving said converted plurality of single-port packets from said selected one of the plurality of different commonly-open TCP ports;

a second conversion table for reconverting said converted plurality of single-port packets into said multipoint communication protocol, resulting in a reconverted plurality of multipoint packets; and

wherein said second interface distributes each of said reconverted plurality of multipoint packets to said two or more ports for communication to said at least a second endpoint communication device; and

wherein one or more firewalls are traversed between said first and second network devices using said selected one of the plurality of different commonly-open TCP ports.

15. The system of claim 14, further comprising:

an encryption application in said first network device for encrypting said plurality of packets in said single-port communication protocol; and

a decryption application in said second network device for decrypting said encrypted plurality of packets prior to said reconverting.

16. The system of claim 15, wherein said encrypting is according to one of:

an Advanced Encryption Standard (AES) 128-bit algorithm;

a Triple Data Encryption Standard (TDES) algorithm; or a Skipjack algorithm.

17. The system of claim 14, wherein said single-port communication protocol is Secure Sockets Layer (SSL) protocol.

18. The system of claim 14, wherein:

a portion of said plurality of packets from said two or more ports conform to Transmission Control Protocol (TCP); another portion of said plurality of packets from said two or more ports conform to User Datagram Protocol (UDP); and

wherein said single-port communication protocol uses said TCP.

19. The system of claim 14, wherein said first and second network devices send alternate data instead of requested data in response to a resend request.

20. The system of claim 14, wherein said first network device qualifies said multipoint packets, wherein said qualifying comprises:

registering a third network device with said first network device;

using network ports by said third network device;

## US 7,710,978 B2

## 11

determining whether said plurality of multiport packets originated from a network port used by said third network device; and

allowing further transmission of said plurality of multiport packets based on said determining. 5

**21.** The system of claim **14**, wherein said selected one of the plurality of different commonly-open TCP ports is a well-known port.

**22.** The system of claim **14**, wherein said selected one of the plurality of different commonly-open TCP ports is port **443**. 10

**23.** A method comprising:

receiving, at a first intermediary network device that is communicatively coupled with a source communication device, a plurality of multiport packets of data from two or more ports for communication from said source communication device, said plurality of multiport packets having at least one original communication protocol; 15

encrypting the plurality of multiport packets, thereby resulting in encrypted packets; 20

encapsulating the encrypted packets into a plurality of single-port packets in a single-port communication protocol that is acceptable by any of a plurality of different commonly-open ports, thereby resulting in encapsulated packets; 25

transmitting from said first intermediary network device said encapsulated packets over a selected one of the plurality of different commonly-open ports, wherein said encapsulated packets traverse one or more firewalls between said first intermediary network device and a second intermediary network device using said selected one of the plurality of different commonly-open ports; 30

receiving, at said second intermediary network device that is communicatively coupled with a destination communication device, said encapsulated packets from said selected one of the plurality of different commonly-open ports; 35

decrypting the received encapsulated packets, thereby resulting in decrypted packets; 40

## 12

restoring the decrypted packets to the at least one original communication protocol, thereby resulting in restored multiport packets; and

distributing, from said second intermediary network device, each of said restored multiport packets to said two or more ports for communication to said destination communication device.

**24.** The method of claim **23**, wherein said encrypting is according to one of:

an Advanced Encryption Standard (AES) 128-bit algorithm;

a Triple Data Encryption Standard (TDES) algorithm; or  
a Skipjack algorithm.

**25.** The method of claim **23**, wherein said single-port communication protocol is Secure Sockets Layer (SSL) protocol.

**26.** The method of claim **23**, wherein:

a portion of said plurality of multiport packets from said two or more ports conform to Transmission Control Protocol (TCP);

another portion of said plurality of multiport packets from said two or more ports conform to User Datagram Protocol (UDP); and

wherein said single-port communication protocol uses said TCP.

**27.** The method of claim **23**, wherein said first and second intermediary network devices send alternate data instead of requested data in response to a resend request.

**28.** The method of claim **23**, further comprising qualifying said multiport packets, wherein said qualifying comprises:

registering a third network device with said first intermediary network device;

determining whether said plurality of multiport packets originated from said third network device; and

allowing further transmission of said plurality of multiport packets based on said determining.

**29.** The method of claim **23**, wherein said selected one of the plurality of different commonly-open ports is a well-known port.

**30.** The method of claim **23**, wherein said selected one of the plurality of different commonly-open ports is port **443**. 40

\* \* \* \* \*

# **EXHIBIT 3**

(12) **United States Patent**  
**Signaoff et al.**

(10) **Patent No.: US 7,773,588 B2**  
(45) **Date of Patent: Aug. 10, 2010**

(54) **SYSTEM AND METHOD FOR CROSS  
PROTOCOL COMMUNICATION**

(75) Inventors: **Christopher S. Signaoff**, Hutto, TX  
(US); **Tom W. Opsahl**, Flower Mound,  
TX (US); **Edward M. Riley, III**, Flower  
Mound, TX (US); **Justin S. Signaoff**,  
Round Rock, TX (US)

(73) Assignee: **directPacket Research, Inc.**, Irving, TX  
(US)

(\*) Notice: Subject to any disclaimer, the term of this  
patent is extended or adjusted under 35  
U.S.C. 154(b) by 579 days.

|                |         |                    |
|----------------|---------|--------------------|
| 6,735,626 B1   | 5/2004  | Tezuka et al.      |
| 6,795,444 B1   | 9/2004  | Vo et al.          |
| 6,798,782 B1   | 9/2004  | Caronni et al.     |
| 6,963,583 B1 * | 11/2005 | Foti ..... 370/467 |
| 7,016,935 B2   | 3/2006  | Lee et al.         |
| 7,020,130 B2   | 3/2006  | Krause et al.      |
| 7,023,465 B2   | 4/2006  | Stephens, Jr.      |
| 7,031,341 B2   | 4/2006  | Yu                 |
| 7,039,701 B2   | 5/2006  | Wesley             |
| 7,159,036 B2   | 1/2007  | Hinchliffe et al.  |

(Continued)

(21) Appl. No.: **11/403,552**

**OTHER PUBLICATIONS**

(22) Filed: **Apr. 13, 2006**

International Search Report and Written Opinion issued for PCT/  
US07/66457 dated Jun. 17, 2008, 10 pgs.

(65) **Prior Publication Data**  
US 2007/0242694 A1 Oct. 18, 2007

(Continued)

(51) **Int. Cl.**  
**H04L 12/66** (2006.01)  
**H04L 12/56** (2006.01)  
**H04J 3/22** (2006.01)  
**G06F 15/16** (2006.01)

*Primary Examiner*—Tri H Phan  
(74) *Attorney, Agent, or Firm*—Fulbright & Jaworski L.L.P.

(52) **U.S. Cl.** ..... **370/356; 370/401; 370/467;**  
709/227

(58) **Field of Classification Search** ..... 370/352–356,  
370/401–408, 466–467; 709/227–228  
See application file for complete search history.

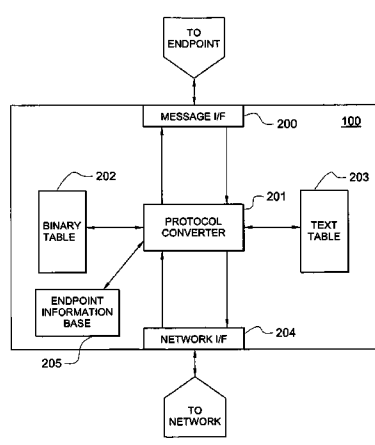
(57) **ABSTRACT**

A multimedia communication system and method are described where a communication controller receives a multimedia data stream from a communication device in a first protocol. The controller detects a type of the first protocol, such as text-based protocol or a binary protocol and then converts the first protocol into an intermediate protocol. The multimedia data stream in this intermediate protocol is then transmitted to a second communication controller connected to the destination communication device. The multimedia data stream is then converted at the second communication controller from the intermediate protocol into a second protocol which is then used to transmit the multimedia data stream to the destination communication device.

(56) **References Cited**  
**U.S. PATENT DOCUMENTS**

|                |         |                            |
|----------------|---------|----------------------------|
| 6,047,320 A    | 4/2000  | Tezuka et al.              |
| 6,266,809 B1   | 7/2001  | Craig et al.               |
| 6,380,968 B1   | 4/2002  | Alexander et al.           |
| 6,434,140 B1 * | 8/2002  | Barany et al. .... 370/352 |
| 6,611,503 B1   | 8/2003  | Fitzgerald et al.          |
| 6,614,465 B2   | 9/2003  | Alexander et al.           |
| 6,633,324 B2   | 10/2003 | Stephens, Jr.              |
| 6,633,985 B2   | 10/2003 | Drell                      |

**23 Claims, 7 Drawing Sheets**





## US 7,773,588 B2

Page 2

## U.S. PATENT DOCUMENTS

|                   |         |                    |                   |         |                 |         |
|-------------------|---------|--------------------|-------------------|---------|-----------------|---------|
| 7,177,929 B2      | 2/2007  | Burbeck et al.     | 2005/0243747 A1 * | 11/2005 | Rudolph         | 370/282 |
| 7,181,530 B1      | 2/2007  | Halasz et al.      | 2005/0259145 A1   | 11/2005 | Schrader et al. |         |
| 7,194,526 B2      | 3/2007  | Kanemitsu          | 2005/0271051 A1   | 12/2005 | Holloway et al. |         |
| 7,206,808 B2      | 4/2007  | Babka et al.       | 2006/0098684 A1 * | 5/2006  | Bozzonek et al. | 370/466 |
| 7,251,689 B2      | 7/2007  | Wesley             | 2006/0104288 A1   | 5/2006  | Yim et al.      |         |
| 7,293,169 B1      | 11/2007 | Righi et al.       | 2006/0109862 A1   | 5/2006  | Choi et al.     |         |
| 7,328,406 B2      | 2/2008  | Kalinoski et al.   | 2006/0187903 A1 * | 8/2006  | Kallio et al.   | 370/352 |
| 7,346,076 B1 *    | 3/2008  | Habiby et al.      | 2006/0190719 A1   | 8/2006  | Rao et al.      |         |
| 7,346,912 B2      | 3/2008  | Seebaldt           | 2006/0224883 A1   | 10/2006 | Khosravi et al. |         |
| 7,353,380 B2      | 4/2008  | VanHeyningen       | 2007/0005804 A1   | 1/2007  | Rideout         |         |
| 7,363,381 B2      | 4/2008  | Mussman et al.     | 2007/0022201 A1   | 1/2007  | Aaby et al.     |         |
| 7,370,097 B2      | 5/2008  | Hashimoto          | 2007/0036143 A1   | 2/2007  | Alt et al.      |         |
| 7,372,957 B2      | 5/2008  | Strathmeyer et al. | 2007/0239841 A1   | 10/2007 | Lehrman         |         |
| 7,385,622 B2      | 6/2008  | Babka et al.       | 2007/0242696 A1   | 10/2007 | Signaoff et al. |         |
| 7,436,428 B2      | 10/2008 | Schrader et al.    | 2008/0043091 A1   | 2/2008  | Lia et al.      |         |
| 7,441,270 B1      | 10/2008 | Edwards et al.     | 2008/0134200 A1   | 6/2008  | Seebaldt        |         |
| 2003/0065737 A1   | 4/2003  | Aasman             | 2008/0235362 A1   | 9/2008  | Kjesbu et al.   |         |
| 2003/0081783 A1   | 5/2003  | Adusumilli et al.  | 2009/0051752 A1   | 2/2009  | Lammers         |         |
| 2003/0182451 A1   | 9/2003  | Grass et al.       | 2009/0112671 A1   | 4/2009  | Grodum          |         |
| 2003/0227908 A1 * | 12/2003 | Scoggins et al.    |                   |         |                 |         |
| 2003/0232648 A1   | 12/2003 | Prindle            |                   |         |                 |         |
| 2004/0037268 A1   | 2/2004  | Read               |                   |         |                 |         |
| 2004/0158606 A1   | 8/2004  | Tsai               |                   |         |                 |         |
| 2005/0021610 A1   | 1/2005  | Bozzonek et al.    |                   |         |                 |         |
| 2005/0080919 A1   | 4/2005  | Li et al.          |                   |         |                 |         |
| 2005/0122964 A1   | 6/2005  | Strathmeyer et al. |                   |         |                 |         |
| 2005/0125696 A1 * | 6/2005  | Afshar et al.      |                   |         |                 |         |

## OTHER PUBLICATIONS

International Search Report and Written Opinion issued for PCT/US2007/066435; Dated: Apr. 2, 2008; 9 Pages.  
 International Search Report and Written Opinion issued for PCT/US2007/066451; Dated: Jul. 7, 2008; 11 Pages.  
 International Search Report and Written Opinion issued for PCT/US2007/066460; Dated: Apr. 9, 2008; 10 Pages.

\* cited by examiner

FIG. 1A

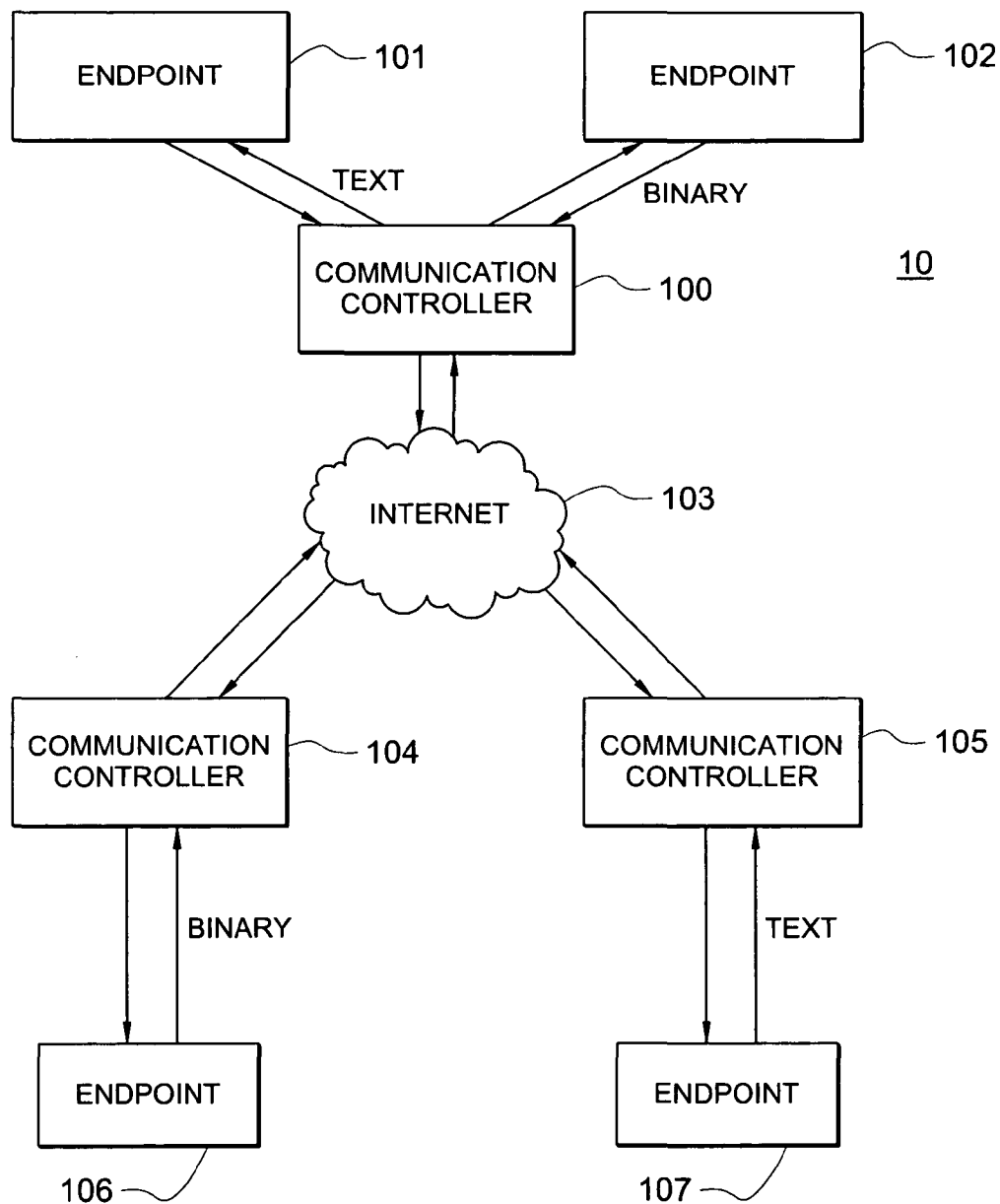


FIG. 1B

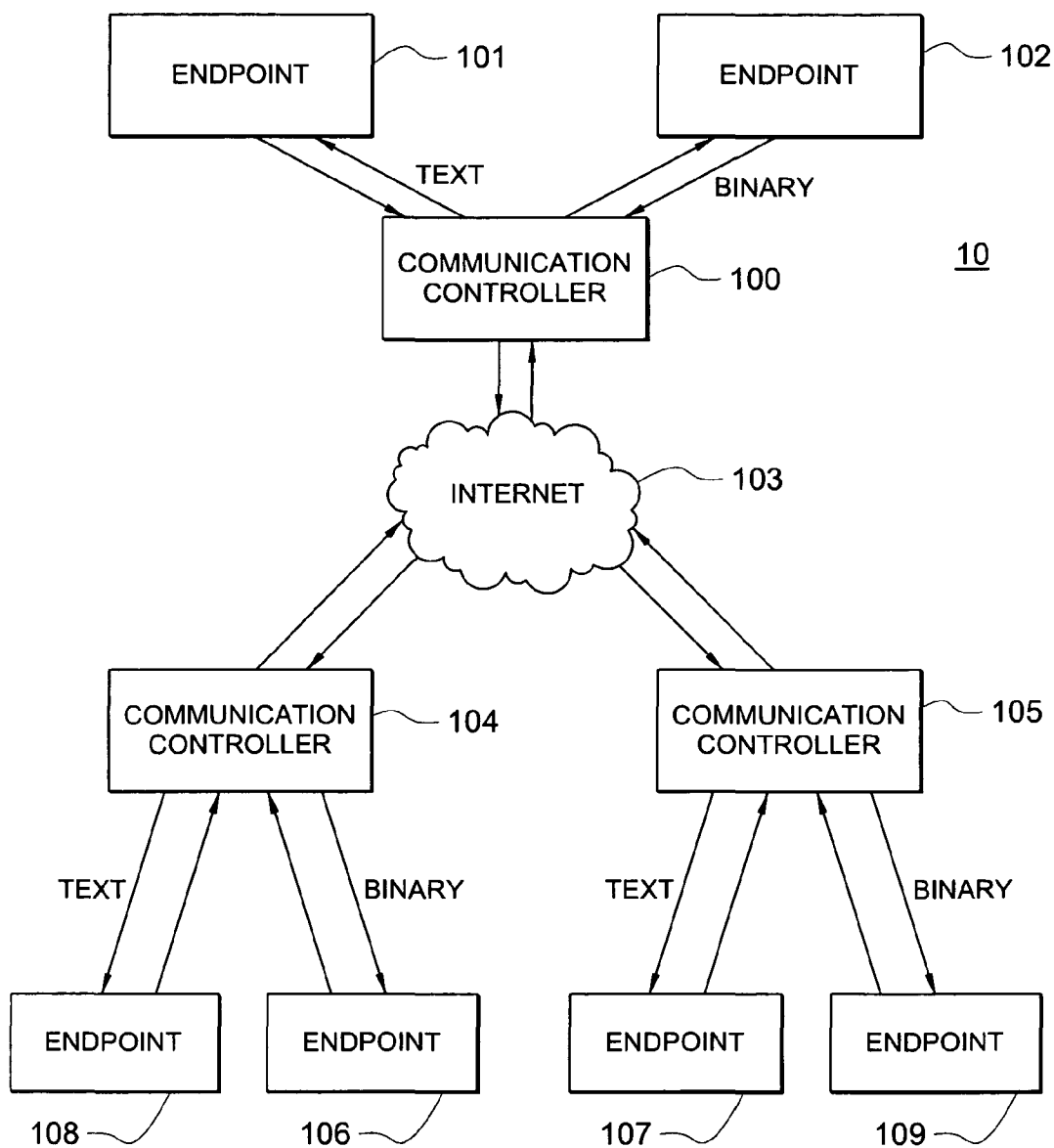


FIG. 2

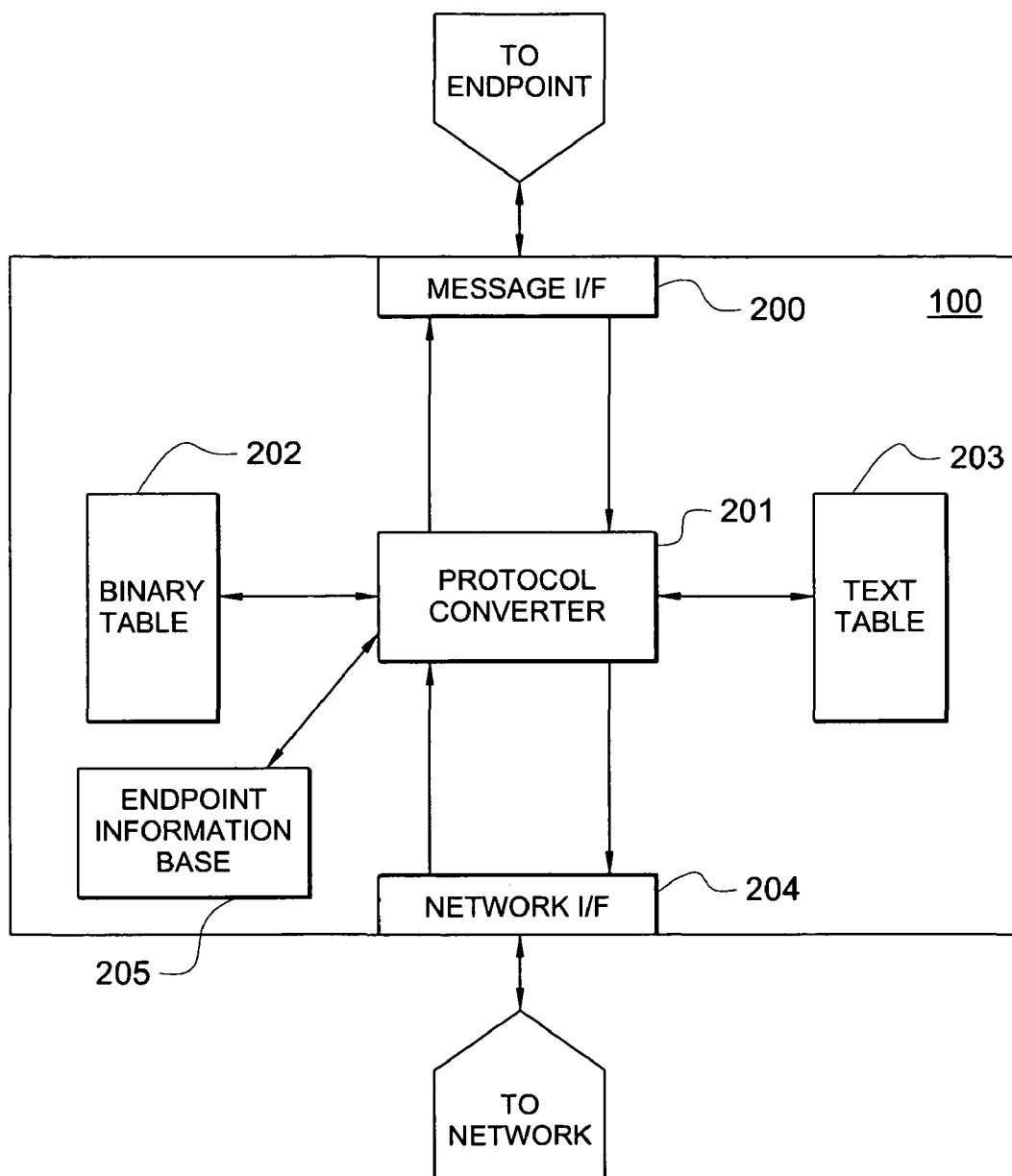
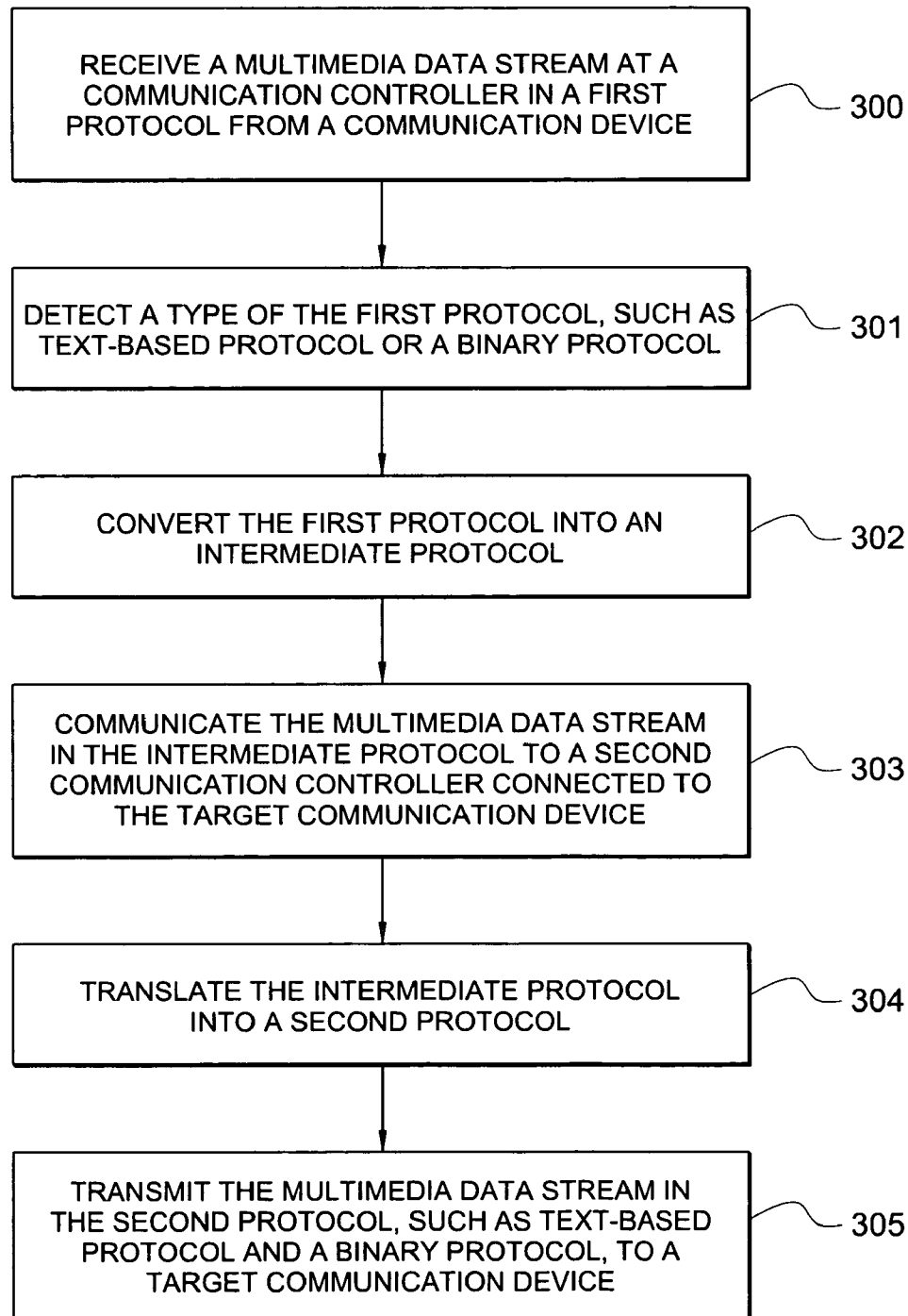
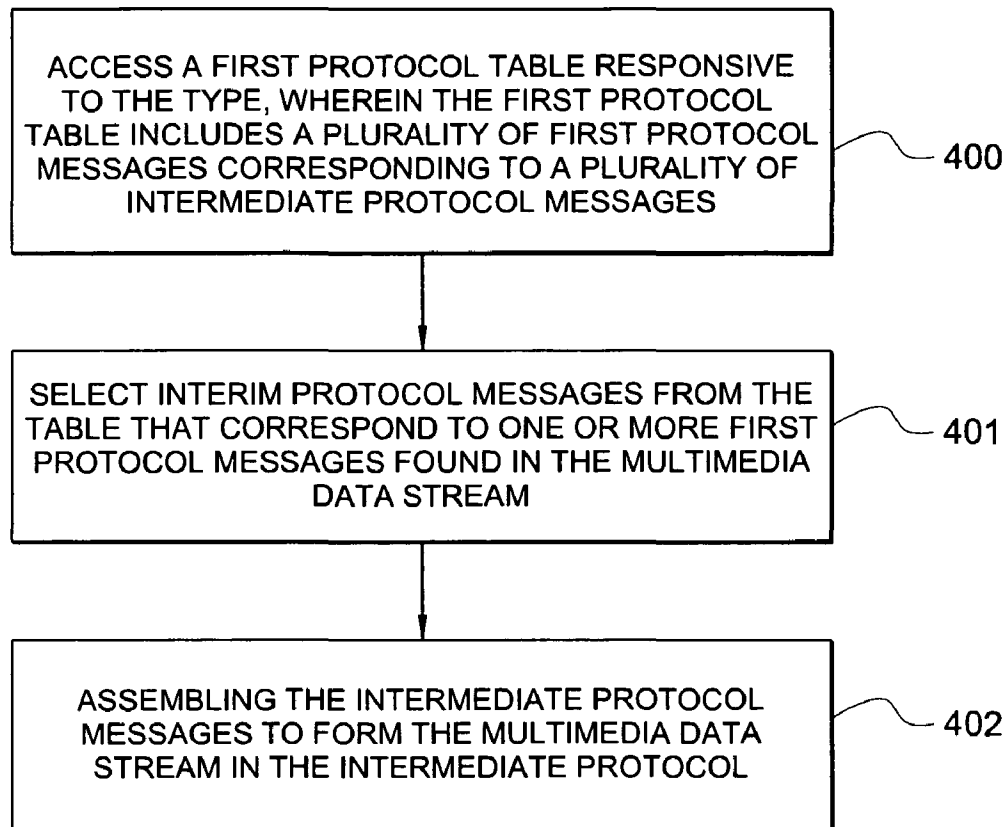


FIG. 3



*FIG. 4*



*FIG. 5*

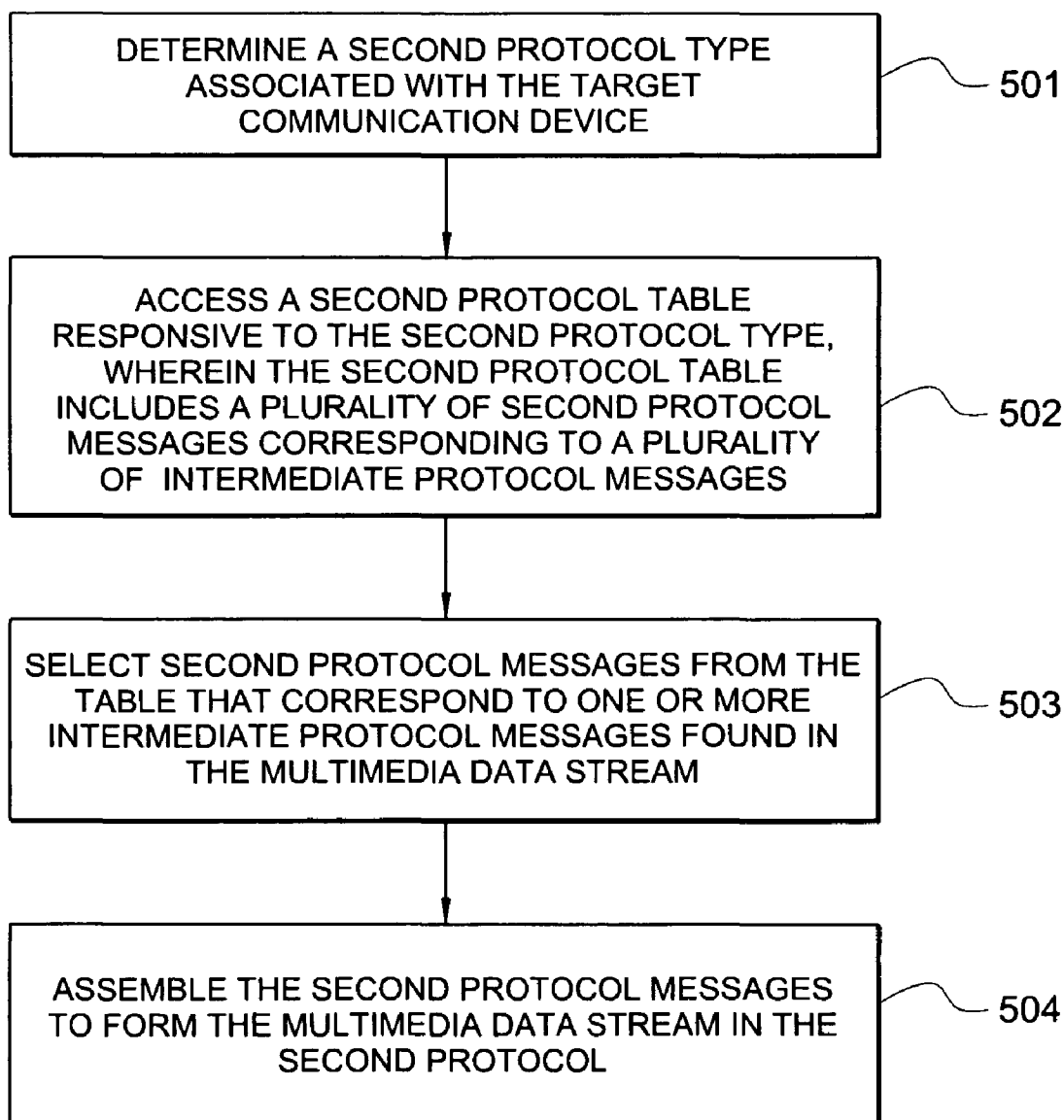
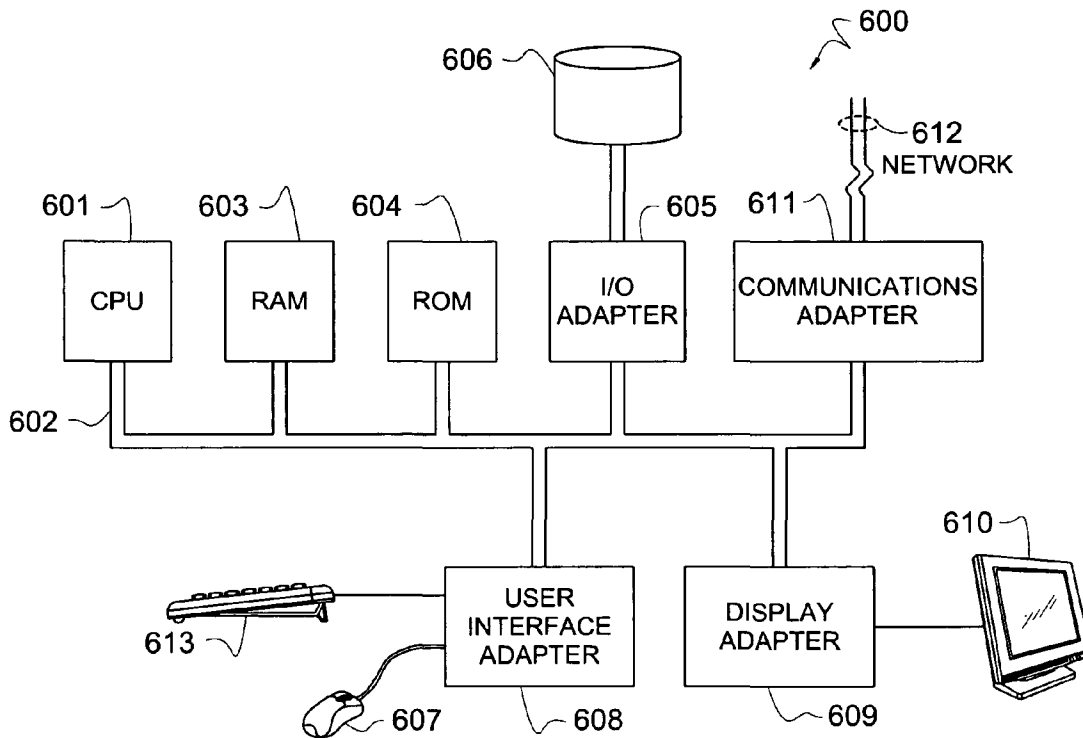


FIG. 6





US 7,773,588 B2

1

**SYSTEM AND METHOD FOR CROSS  
PROTOCOL COMMUNICATION****TECHNICAL FIELD**

The present invention is related to electronic communications systems and, more particularly, to communication using incompatible communication protocols.

**BACKGROUND OF THE INVENTION**

The Internet may be used for many forms of communication, including voice conversations, video conferencing, development collaboration, and the like. In order for a manufacturers' programs, applications, equipment, and systems to be interoperable with each other, many protocols have been developed to standardize the communication between such systems. These protocols have grown increasingly complex to handle all the types of traffic generated to facilitate communication for video conferencing, voice over Internet Protocol (VoIP), and data over Internet Protocol applications. Two examples of such protocols that have been defined for handling the administration of VoIP, and its natural extension to multimedia communication are H.323 from the International Telecommunication Union-Telecommunication Standardization Sector (ITU-T) and the Session Initiation Protocol (SIP) from the Internet Engineering Task Force (IETF). Both H.323 and SIP typically allow for multimedia communication including voice, video, and data communications in real-time.

H.323 and SIP, in addition to other such communication protocols, each rely on multiple other protocols, some of which may in turn rely on UDP for sending and receiving multimedia traffic. UDP features minimal overhead compared to other transport protocols (most notably TCP) at the expense of having less reliability. UDP does not provide for guaranteed packet delivery nor data integrity. UDP does offer the highest possible throughput, thus, making it ideally suited for multimedia real-time communications.

While these different protocols, such as H.323 and SIP, each facilitate the multimedia communication, they are quite different in structure and format. Some protocols, such as H.323, are binary format protocols. That means the transmitted information in the H.323 stream is in a binary coded format. In contrast, other protocols, such as SIP, are text-based protocols, which means that text tags or other information are included in the transmitted streams. Multimedia communication systems, therefore, are typically designed to be implemented in one of the various protocols. For example, one communication system may be designed to operate with H.323, while others might be designed to operate with SIP, VoIP, or the like.

A problem arises when a party using an H.323 endpoint on one communication system designed to use H.323 desires to communicate with another party using a different protocol endpoint on another communication system designed for the different protocol. Because the two systems and endpoints use incompatible protocols, communication cannot be established between the two parties by connecting the first endpoint and system with the target endpoint and system. The two endpoints and systems speak different languages and, thus, cannot understand the messaging and data being transmitted by the other. As the popularity of Internet-based or electronic multimedia communications grows, a likelihood exists that this problem may be encountered with increasing frequency.

2

**BRIEF SUMMARY OF THE INVENTION**

The present invention is directed to a system and method for facilitating multimedia communication with multiple communication protocols. A communication controller within the system receives a multimedia data stream in a first protocol from a communication device. The controller detects a type of the first protocol, such as text-based protocol or a binary protocol, and converts the first protocol into an intermediate protocol. The intermediate protocol may be created to reflect the commonalities between the various communication protocols that are expected within the system. The multimedia data stream in this intermediate protocol is then transmitted to a second communication controller connected to the target communication device. The second communication controller converts the multimedia data stream in the intermediate protocol into a second protocol that is compatible with the destination communication device. Prior to making this conversion, the second communication controller would determine what protocol this destination device uses. The multimedia data stream in this second protocol is then transmitted to the destination communication device. By providing the interim or intermediate protocol, translation or conversion between the different protocols is quick and efficient. Moreover, it allows communication devices that use different communication protocols to participate in multimedia communications on the same system.

The foregoing has outlined rather broadly the features and technical advantages of the present invention in order that the detailed description of the invention that follows may be better understood. Additional features and advantages of the invention will be described hereinafter which form the subject of the claims of the invention. It should be appreciated by those skilled in the art that the conception and specific embodiment disclosed may be readily utilized as a basis for modifying or designing other structures for carrying out the same purposes of the present invention. It should also be realized by those skilled in the art that such equivalent constructions do not depart from the spirit and scope of the invention as set forth in the appended claims. The novel features which are believed to be characteristic of the invention, both as to its organization and method of operation, together with further objects and advantages will be better understood from the following description when considered in connection with the accompanying figures. It is to be expressly understood, however, that each of the figures is provided for the purpose of illustration and description only and is not intended as a definition of the limits of the present invention.

**BRIEF DESCRIPTION OF THE DRAWINGS**

For a more complete understanding of the present invention, reference is now made to the following descriptions taken in conjunction with the accompanying drawing, in which:

FIG. 1A is a block diagram illustrating a multimedia communication network configured according to one embodiment of the present invention;

FIG. 1B is a block diagram illustrating the multimedia communication network of FIG. 1A in an alternative connection;

FIG. 2 is a detailed block diagram illustrating component blocks of a communication controller;

FIG. 3 is a flowchart illustrating example steps executed to implement one embodiment of the present invention;

US 7,773,588 B2

3

FIG. 4 is a flowchart illustrating example steps executed to convert a first protocol into an intermediate protocol in a multimedia communication system configured according to one embodiment of the present invention;

FIG. 5 is a flowchart illustrating example steps executed to convert an intermediate protocol into a second protocol in a multimedia communication system configured according to one embodiment of the present invention; and

FIG. 6 illustrates a computer system adapted to use embodiments of the present invention.

#### DETAILED DESCRIPTION OF THE INVENTION

FIG. 1A is a block diagram illustrating multimedia communication network 10 configured according to one embodiment of the present invention. Multimedia communication network 10 includes communication controller 100 connected to endpoints 101 and 102. Communication controller 100 is also connected to Internet 103 to facilitate connections with communication controllers 104 and 105, and endpoints 106 and 107. A major difference between multimedia communication network 10 and other existing communication networks is that endpoints 101-102 and 106-107 communicate using different communication protocols.

Endpoints 101 and 107 each use a text-based communication protocol, such as SIP, while endpoints 102 and 106 each use a binary communication protocol, such as H.323. SIP and H.323 are merely specific examples of text-based and binary protocols. Other protocols may be used as well. Because the binary communication protocol is incompatible with the text-based protocol, endpoint 101 cannot directly communicate with endpoint 102 simply by sending its communication stream to endpoint 102. Instead, communication controller 100 receives the multimedia communication stream from endpoint 101 in the text-based protocol and converts it line-by-line into an interim protocol that comprises the common functions and elements of the different protocols. Communication controller 100 then converts the interim protocol into the binary protocol for transmission to endpoint 102.

In implementing multimedia communication between multiple endpoints connected at various remote locations with different communication controllers, the transmitting communication controller translates the text-based or binary communication protocol into an interim or intermediate communication protocol that simplifies the protocol signals into their common elements. This intermediate communication protocol may be efficiently transmitted across Internet 103 to either or both of communication controllers 104 and 105. Once received at communication controllers 104 and 105, the intermediate communication protocol is then converted into the appropriate communication protocol for delivery to endpoints 106 and 107 (i.e., binary for endpoint 106 and text-based for endpoint 107). This conversion process, thus, allows multiple endpoints that communicate using different communication protocols to communicate effectively within the single multimedia communication system 10.

It should be noted that in additional and alternative embodiments of the present invention, any different type of communication protocol may be used by the various endpoints. Moreover, the communication controllers may be configured to service any number of different endpoints.

FIG. 1B is a block diagram illustrating multimedia communication network 10 in an alternative connection session. As described in FIG. 1A, communication from endpoints 101 and 102 are converted from a text-based protocol and a binary protocol (respectively), into the interim or intermediate protocol which is then transmitted to the destination endpoints.

4

In the connection illustrated in FIG. 1B, more endpoints, endpoints 108 and 109, are connected into multimedia communication network 10 through communication controllers 104 and 105. Endpoint 108, connected to communication controller 104, communicates using a text-based protocol, which is different than the binary protocol used by endpoint 106. Similarly, endpoint 109 communicates using a binary protocol, which is different from the text-based protocol of endpoint 107, both of which are connected to communication controller 105. The various embodiments of the present invention allow any of the endpoints connected into a communication controller to transmit its multimedia communication data in various, incompatible protocols. In this manner, the intermediate protocol data stream arriving at communication controller 104 will be converted into a text-based protocol for delivery to endpoint 108, and will also be converted into a binary protocol for delivery to endpoint 106. Thus, the protocol of the endpoint does not limit the communication within multimedia communication network 10.

FIG. 2 is a detailed block diagram illustrating component blocks of communication controller 100. When initiating multimedia communications, an endpoint transmits the multimedia data streams to communication controller 100 in the communication protocol that it was configured for. Communication controller 100 receives the data streams at message interface 200. Message interface 200 sends the data stream to protocol converter 201. Protocol converter 201 examines the data stream and first determines what protocol the data stream has been configured for. With this information, protocol converter 201 begins examining the data stream packets to find protocol messages or commands contained within the data stream. As such protocol messages or commands are found, protocol converter 201 accesses a corresponding table to find the interim protocol message to replace the original message.

In the example depicted in FIG. 2, protocol converter 201 may access binary table 202, when the received multimedia data stream is in a binary format protocol, or it may access text table 203, when the received multimedia data stream is in a text-based protocol. For purposes of this example, the endpoint is transmitting a data stream in a text-based protocol. Therefore, protocol converter 201 accesses text table 203 when it discovers messages or commands in the text-based protocol. Protocol converter 201 searches through text table 203 for messages or commands in the interim protocol that correspond to the message or command discovered in the original, text-based protocol. Protocol converter 201 begins translating the data stream line-by-line into a new, interim data stream by retrieving the associated message or command in the interim protocol from text table 203 and packaging the payload or data from the original data stream along with the message or command in the interim protocol.

As protocol converter 201 assembles the new data stream in the interim protocol, the stream is forwarded to network interface 204 for transmission of the translated data stream onto the network. The translated interim data stream will be addressed to any of the target endpoints by way of any intervening communication controllers.

Protocol converter 100 also works in reverse upon the receipt of a communication data stream from the network. The data stream is received at network interface 204 in the interim protocol. Network interface 204 sends the data stream to protocol converter 201. As a part of the interim data stream, the address of the target endpoint is included in the stream administrative data. Protocol converter 201 parses this administrative data from the stream and locates information on the target endpoint by accessing endpoint information base 205. Endpoint information base 205 maintains records

US 7,773,588 B2

5

of the capabilities and compatibilities of each of the endpoints connected to communication controller **100**. One such capability is the type of communication protocol that the target endpoint speaks. With this information, protocol converter **201** accesses either binary table **202** or text table **203**, depending on which protocol the endpoint understands. Protocol converter **201** then begins scanning the interim data stream for the commands and messages in the interim protocol.

For purposes of this example, the target endpoint uses a binary formatted protocol. Therefore, protocol converter **201** accesses binary table **202** and locates the binary protocol messages or commands that correspond to the interim protocol and begins re-packaging the transferred data into a multimedia data stream in the binary protocol. As the new, re-packaged multimedia data stream is being assembled, protocol converter **201** transmits the stream to message interface **200** addressed to the appropriate endpoint attached to communication controller **100**. By performing these conversions in real-time from an efficient interim protocol, the multimedia communication system configured according to an embodiment of the present invention is able to facilitate communication between multiple endpoints even though those endpoints are not configured to receive the same communication protocol. Moreover, because an interim protocol is used to transmit the data stream between protocol converters in the network, the conversion to the ultimate communication protocol at the protocol converter connected to the target endpoint, thus, improving the conversion speed and efficiency of the communication.

FIG. 3 is a flowchart illustrating example steps executed to implement one embodiment of the present invention. In step **300**, a multimedia data stream is received from a communication device at a communication controller in a first protocol. In step **301**, a type of the first protocol, such as text-based protocol or a binary protocol, is detected. The first protocol is converted into an intermediate protocol in step **302**. The multimedia data stream in the intermediate protocol is communicated, in step **303**, to a second communication controller connected to the target communication device. The intermediate protocol is translated into a second protocol in step **304**. In step **305**, the multimedia data stream in the second protocol, such as text-based protocol and a binary protocol, is transmitted to a target communication device.

In converting a first protocol into the interim or intermediate protocol, steps are executed to translate the protocol of the data stream line-by-line or bit-by-bit. FIG. 4 is a flowchart illustrating example steps executed to convert a first protocol into an intermediate protocol according to one embodiment of the present invention. In step **400**, a first protocol table is accessed responsive to the type of protocol detected. The first protocol table includes first protocol messages and shows the corresponding intermediate protocol messages. Interim protocol messages are selected, in step **401**, from the table that correspond to the first protocol messages in the multimedia data stream. In step **402**, the intermediate protocol messages are assembled to form the multimedia data stream in the intermediate protocol. The assembled message is then transmitted onto the network for communication.

The multimedia data stream received in the interim or intermediate protocol is also converted line-by-line or bit-by-bit into the protocol appropriate for the target or destination endpoint or communication device. FIG. 5 is a flowchart illustrating example steps executed to convert an intermediate protocol into a second protocol in a multimedia communication system configured according to one embodiment of the present invention. In step **500**, a second protocol type associated with the target communication device is determined. A

6

second protocol table is accessed in step **501** responsive to determination of the second protocol type. The second protocol table includes second protocol messages shown with their corresponding intermediate protocol messages. In step **502**, second protocol messages are selected from the table that correspond to the intermediate protocol messages found in the multimedia data stream. The second protocol messages are assembled, in step **503**, to form the multimedia data stream in the second protocol, which is then forwarded to the destination endpoint or communication device for delivery.

It should be noted that the various embodiments of the present invention are directed to multimedia communication systems. Multimedia communication systems include such multi-format data such as voice and video; voice, video, and data; and the like. Systems that are purely intended to transfer data only, or voice only, may benefit from the techniques described herein. However, the complexities of dealing with the multiple data types in multimedia systems along with the multiple protocols designed for such systems resolves a growing problem which has yet to be addressed in technology.

The program or code segments making up the various embodiments of the present invention may be stored in a computer readable medium or transmitted by a computer data signal embodied in a carrier wave, or a signal modulated by a carrier, over a transmission medium. The "computer readable medium" may include any medium that can store or transfer information. Examples of the computer readable medium include an electronic circuit, a semiconductor memory device, a ROM, a flash memory, an erasable ROM (EROM), a floppy diskette, a compact disk CD-ROM, an optical disk, a hard disk, a fiber optic medium, a radio frequency (RF) link, and the like. It may also include fixed or reprogrammable ROM used as firmware for various hardware devices. The computer data signal may include any signal that can propagate over a transmission medium such as electronic network channels, optical fibers, air, electromagnetic, RF links, and the like. The code segments may be downloaded via computer networks such as the Internet, Intranet, and the like.

FIG. 6 illustrates computer system **600** adapted to use embodiments of the present invention, e.g. storing and/or executing software associated with the embodiments. Central processing unit (CPU) **601** is coupled to system bus **602**. The CPU **601** may be any general purpose CPU. However, embodiments of the present invention are not restricted by the architecture of CPU **601** as long as CPU **601** supports the inventive operations as described herein. Bus **602** is coupled to random access memory (RAM) **603**, which may be SRAM, DRAM, or SDRAM. ROM **604** is also coupled to bus **602**, which may be PROM, EPROM, or EEPROM. RAM **603** and ROM **604** hold user and system data and programs as is well known in the art.

Bus **602** is also coupled to input/output (I/O) controller card **605**, communications adapter card **611**, user interface card **608**, and display card **609**. The I/O adapter card **605** connects storage devices **606**, such as one or more of a hard drive, a CD drive, a floppy disk drive, a tape drive, to computer system **600**. The I/O adapter **605** is also connected to a printer (not shown), which would allow the system to print paper copies of information such as documents, photographs, articles, and the like. Note that the printer may be a printer (e.g., dot matrix, laser, and the like), a fax machine, scanner, or a copier machine. Communications card **611** is adapted to couple the computer system **600** to a network **612**, which may be one or more of a telephone network, a local (LAN) and/or a wide-area (WAN) network, an Ethernet network, and/or the Internet network. User interface card **608** couples user input

## US 7,773,588 B2

7

devices, such as keyboard **613**, pointing device **607**, and the like, to the computer system **600**. The display card **609** is driven by CPU **601** to control the display on display device **610**.

Although the present invention and its advantages have been described in detail, it should be understood that various changes, substitutions and alterations can be made herein without departing from the spirit and scope of the invention as defined by the appended claims. Moreover, the scope of the present application is not intended to be limited to the particular embodiments of the process, machine, manufacture, composition of matter, means, methods and steps described in the specification. As one of ordinary skill in the art will readily appreciate from the disclosure of the present invention, processes, machines, manufacture, compositions of matter, means, methods, or steps, presently existing or later to be developed that perform substantially the same function or achieve substantially the same result as the corresponding embodiments described herein may be utilized according to the present invention. Accordingly, the appended claims are intended to include within their scope such processes, machines, manufacture, compositions of matter, means, methods, or steps.

What is claimed is:

1. A method for multimedia communication comprising: receiving a multimedia data stream at a communication controller in a first protocol from a communication device, wherein the first protocol comprises a signaling protocol; detecting a type of said first protocol; converting said first protocol into an intermediate protocol; translating said intermediate protocol into a second protocol, wherein the second protocol comprises a signaling protocol; and transmitting said multimedia data stream in said second protocol to a target communication device; wherein said first protocol comprises one of a text-based protocol and a binary protocol and wherein said second protocol comprises one of a binary protocol and a text-based protocol.
2. The method of claim 1 further comprising: communicating, prior to said translating, said multimedia data stream in said communication controller to a second communication controller connected to said target communication device; wherein said translating and said transmitting are performed by said second communication controller.
3. The method of claim 1 wherein said converting comprises: accessing a first protocol table responsive to said type, wherein said first protocol table includes a plurality of first protocol messages corresponding to a plurality of intermediate protocol messages; selecting ones of said plurality of intermediate protocol messages that correspond to one or more first protocol messages found in said multimedia data stream; and assembling said ones of said plurality of intermediate protocol messages to form said multimedia data stream in said intermediate protocol.
4. The method of claim 1 wherein said translating comprises: determining a second protocol type associated with said target communication device; accessing a second protocol table responsive to said second protocol type, wherein said second protocol table

8

- includes a plurality of second protocol messages corresponding to said plurality of intermediate protocol messages;
- selecting ones of said plurality of second protocol messages that correspond to one or more intermediate protocol messages found in said multimedia data stream; and
- assembling said ones of said plurality of second protocol messages to form said multimedia data stream in said second protocol.
5. The method of claim 4 further comprising: retrieving said second protocol type from a device information base, wherein said device information base contains compatibility information for each device available for said multimedia communication.
6. The method of claim 1 wherein said intermediate protocol comprises protocol messages common to said text-based protocol and said binary protocol.
7. A communication controller in a multimedia communication system, said communication controller comprising: a message interface to transceive multimedia data from a communication endpoint in a first protocol, wherein the first protocol comprises a signaling protocol, and wherein said first protocol is either a text-based protocol or a binary protocol; a protocol signaler to determine a type of said first protocol; a first protocol conversion table that contains a plurality of first protocol messages and a plurality of interim protocol messages, wherein said plurality of interim protocol messages correspond to ones of said plurality of first protocol messages; a protocol conversion utility to convert said first protocol into an interim protocol using said first protocol conversion table; and a network interface to transceive said multimedia data in said interim protocol to a target communication endpoint.
8. The communication controller of claim 7 wherein said protocol conversion utility converts said interim protocol of a received multimedia data stream into a second protocol and wherein said message interface transmits said received multimedia data stream in said second protocol to a destination endpoint connected to said communication controller.
9. The communication controller of claim 8 further comprising: a second protocol conversion table that contains a plurality of second protocol messages and said plurality of interim protocol messages, wherein said plurality of interim protocol messages correspond to ones of said plurality of second protocol messages.
10. The communication controller of claim 8 further comprising: an endpoint information base including compatibility data on one or more communication endpoints connected to said communication controller, wherein said compatibility data includes a device protocol type.
11. A method for multimedia communication comprising: receiving a multimedia data stream at a communication controller in a first protocol from a communication device; detecting a type of said first protocol; converting said first protocol into an intermediate protocol, wherein said converting is performed irrespective of a second protocol in which the multimedia data stream is to be transmitted to a target communication device; translating said intermediate protocol into said second protocol; and

US 7,773,588 B2

9

transmitting said multimedia data stream in said second protocol to the target communication device;  
 wherein said first protocol comprises one of a text-based protocol and a binary protocol and wherein said second protocol comprises one of a binary protocol and a text-based protocol.

**12.** The method of claim **11** further comprising:

communicating, prior to said translating, said multimedia data stream in said communication controller to a second communication controller connected to said target communication device; wherein said translating and said transmitting are performed by said second communication controller.

**13.** The method of claim **11** wherein said converting comprises:

accessing a first protocol table responsive to said type, wherein said first protocol table includes a plurality of first protocol messages corresponding to a plurality of intermediate protocol messages;

selecting ones of said plurality of intermediate protocol messages that correspond to one or more first protocol messages found in said multimedia data stream; and

assembling said ones of said plurality of intermediate protocol messages to form said multimedia data stream in said intermediate protocol.

**14.** The method of claim **11** wherein said translating comprises:

determining a second protocol type associated with said target communication device;

accessing a second protocol table responsive to said second protocol type, wherein said second protocol table includes a plurality of second protocol messages corresponding to said plurality of intermediate protocol messages;

selecting ones of said plurality of second protocol messages that correspond to one or more intermediate protocol messages found in said multimedia data stream; and

assembling said ones of said plurality of second protocol messages to form said multimedia data stream in said second protocol.

**15.** The method of claim **14** further comprising:

retrieving said second protocol type from a device information base, wherein said device information base contains compatibility information for each device available for said multimedia communication.

**16.** The method of claim **11** wherein said intermediate protocol comprises protocol messages common to said text-based protocol and said binary protocol.

**17.** The method of claim **11** wherein said first protocol comprises a signaling protocol, and wherein said second protocol comprises a signaling protocol.

**18.** A computer program product having a computer readable storage medium with computer program logic recorded thereon for multimedia communication, said computer program product comprising:

code for receiving a multimedia data stream at a communication controller in a first protocol from a communication device;

code for detecting a type of said first protocol;

10

code for converting said first protocol into an intermediate protocol, wherein said converting is performed irrespective of a second protocol in which the multimedia data stream is to be transmitted to a target communication device;

code for translating said intermediate protocol into the second protocol; and

code for transmitting said multimedia data stream in said second protocol to the target communication device;

wherein said first protocol comprises one of a text-based protocol and a binary protocol and wherein said second protocol comprises one of a binary protocol and a text-based protocol.

**19.** The computer program product of claim **18** further comprising:

code for communicating, prior to execution of said code for translating, said multimedia data stream in said communication controller to a second communication controller connected to said target communication device; wherein said code for translating and said code for transmitting are executed at said second communication controller.

**20.** The computer program product of claim **18** wherein said code for converting comprises:

code for accessing a first protocol table responsive to said type, wherein said first protocol table includes a plurality of first protocol messages corresponding to a plurality of intermediate protocol messages;

code for selecting ones of said plurality of intermediate protocol messages that correspond to one or more first protocol messages found in said multimedia data stream; and

code for assembling said ones of said plurality of intermediate protocol messages to form said multimedia data stream in said intermediate protocol.

**21.** The computer program product of claim **18** wherein said code for translating comprises:

code for determining a second protocol type associated with said target communication device;

code for accessing a second protocol table responsive to said second protocol type, wherein said second protocol table includes a plurality of second protocol messages corresponding to said plurality of intermediate protocol messages;

code for selecting ones of said plurality of second protocol messages that correspond to one or more intermediate protocol messages found in said multimedia data stream; and

code for assembling said ones of said plurality of second protocol messages to form said multimedia data stream in said second protocol.

**22.** The computer program product of claim **21** further comprising:

code for retrieving said second protocol type from a device information base, wherein said device information base contains compatibility information for each device available for said multimedia communication.

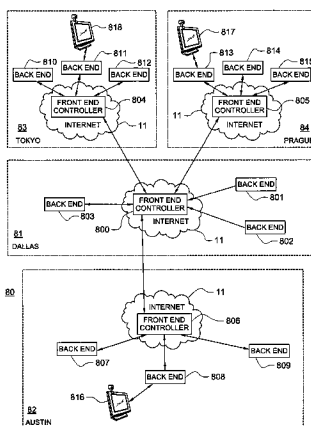
**23.** The computer program product of claim **18** wherein said intermediate protocol comprises protocol messages common to said text-based protocol and said binary protocol.

\* \* \* \* \*

# **EXHIBIT 4**

(10) **Patent No.:** US 8,560,828 B2  
(45) **Date of Patent:** Oct. 15, 2013

- |           |    |         |                   |
|-----------|----|---------|-------------------|
| 5,838,683 | A  | 11/1998 | Corley et al.     |
| 6,047,320 | A  | 4/2000  | Tezuka et al.     |
| 6,266,809 | B1 | 7/2001  | Craig et al.      |
| 6,380,968 | B1 | 4/2002  | Alexander et al.  |
| 6,434,140 | B1 | 8/2002  | Barany et al.     |
| 6,611,503 | B1 | 8/2003  | Fitzgerald et al. |
| 6,614,465 | B2 | 9/2003  | Alexander et al.  |
| 6,633,324 | B2 | 10/2003 | Stephens, Jr.     |
| 6,633,985 | B2 | 10/2003 | Drell             |
| 6,735,626 | B1 | 5/2004  | Tezuka et al.     |
| 6,795,444 | B1 | 9/2004  | Vo et al.         |



**US 8,560,828 B2**

Page 2

---

**23 Claims, 9 Drawing Sheets**



## US 8,560,828 B2

Page 3

(56)

## References Cited

## U.S. PATENT DOCUMENTS

7,251,689 B2 7/2007 Wesley  
 7,254,643 B1 8/2007 Peters, Jr. et al.  
 7,293,169 B1 11/2007 Righi et al.  
 7,328,406 B2 2/2008 Kalinoski et al.  
 7,346,076 B1 3/2008 Habiby et al.  
 7,346,912 B2 3/2008 Seebaldt  
 7,353,380 B2 4/2008 VanHeyningen  
 7,363,381 B2 4/2008 Mussman et al.  
 7,370,097 B2 5/2008 Hashimoto  
 7,372,957 B2 5/2008 Strathmeyer et al.  
 7,385,622 B2 6/2008 Babka et al.  
 7,436,428 B2 10/2008 Schrader et al.  
 7,441,270 B1 10/2008 Edwards et al.  
 7,649,898 B1 1/2010 May, Jr. et al.  
 2001/0043571 A1 11/2001 Jang et al.  
 2001/0046234 A1 11/2001 Agrawal et al.  
 2003/0065737 A1\* 4/2003 Aasman ..... 709/213  
 2003/0081783 A1 5/2003 Adusumilli et al.  
 2003/0182451 A1 9/2003 Grass et al.  
 2003/0227908 A1 12/2003 Scoggins et al.  
 2003/0232648 A1 12/2003 Prindle  
 2004/0037268 A1 2/2004 Read  
 2004/0158606 A1 8/2004 Tsai  
 2005/0021610 A1 1/2005 Bozionek et al.  
 2005/0021772 A1 1/2005 Shedrinsky  
 2005/0080919 A1\* 4/2005 Li et al. .... 709/236  
 2005/0122964 A1\* 6/2005 Strathmeyer et al. .... 370/352  
 2005/0125696 A1 6/2005 Afshar et al.

2005/0141482 A1 6/2005 Kleiner  
 2005/0243747 A1 11/2005 Rudolph  
 2005/0259145 A1 11/2005 Schrader et al.  
 2005/0271051 A1 12/2005 Holloway et al.  
 2006/0098684 A1 5/2006 Bozionek et al.  
 2006/0104288 A1 5/2006 Yim et al.  
 2006/0109862 A1 5/2006 Choi et al.  
 2006/0187903 A1 8/2006 Kallio et al.  
 2006/0190719 A1 8/2006 Rao et al.  
 2006/0224883 A1 10/2006 Khosravi et al.  
 2007/0005804 A1 1/2007 Rideout  
 2007/0022201 A1 1/2007 Aaby et al.  
 2007/0036143 A1\* 2/2007 Alt et al. .... 370/352  
 2007/0239841 A1 10/2007 Lehrman  
 2007/0242696 A1 10/2007 Signaoff et al.  
 2008/0043091 A1 2/2008 Lia et al.  
 2008/0134200 A1 6/2008 Seebaldt  
 2008/0235362 A1 9/2008 Kjesbu et al.  
 2009/0051752 A1 2/2009 Lammers  
 2009/0112671 A1 4/2009 Grodum

## OTHER PUBLICATIONS

International Search Report and Written Opinion issued for PCT/  
 US2007/066435; Dated: Apr. 2, 2008; 9 Pages.  
 International Search Report and Written Opinion issued for PCT/  
 US07/66457 dated Jun. 17, 2008, 10 pgs.  
 International Search Report and Written Opinion issued for PCT/  
 US2007/066460; Dated: Apr. 9, 2008; 10 Pages.

\* cited by examiner

FIG. 1

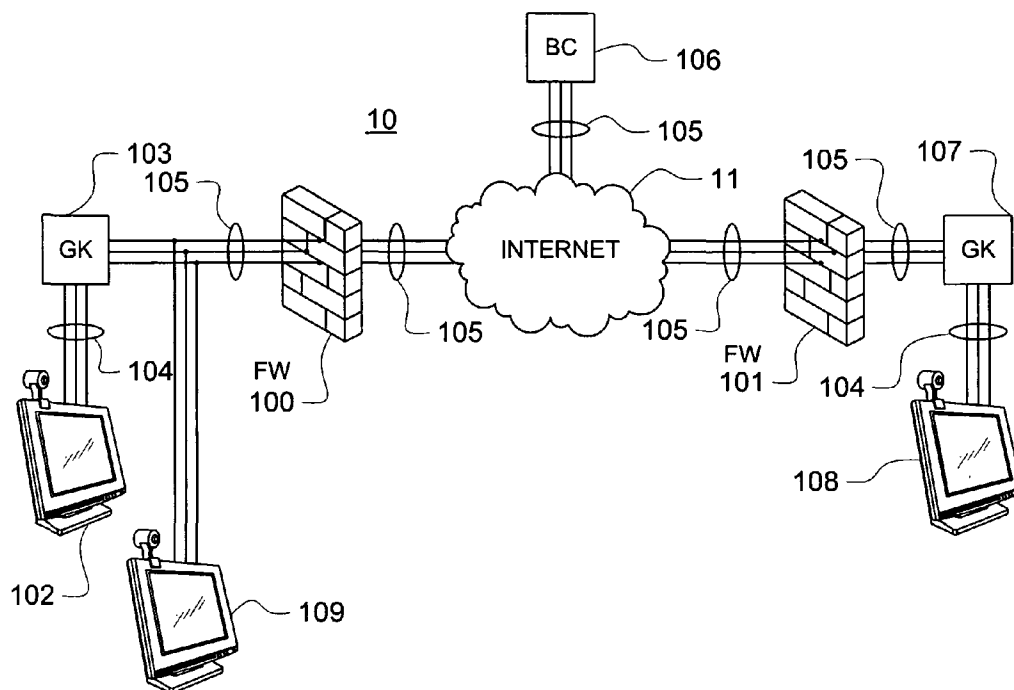


FIG. 3

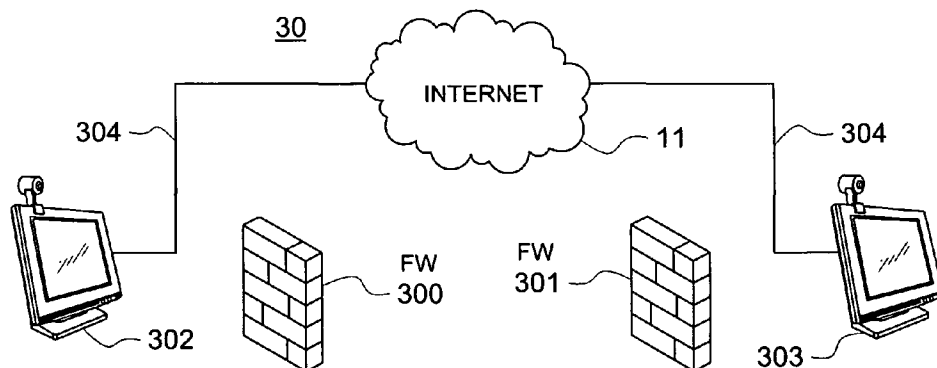


FIG. 2

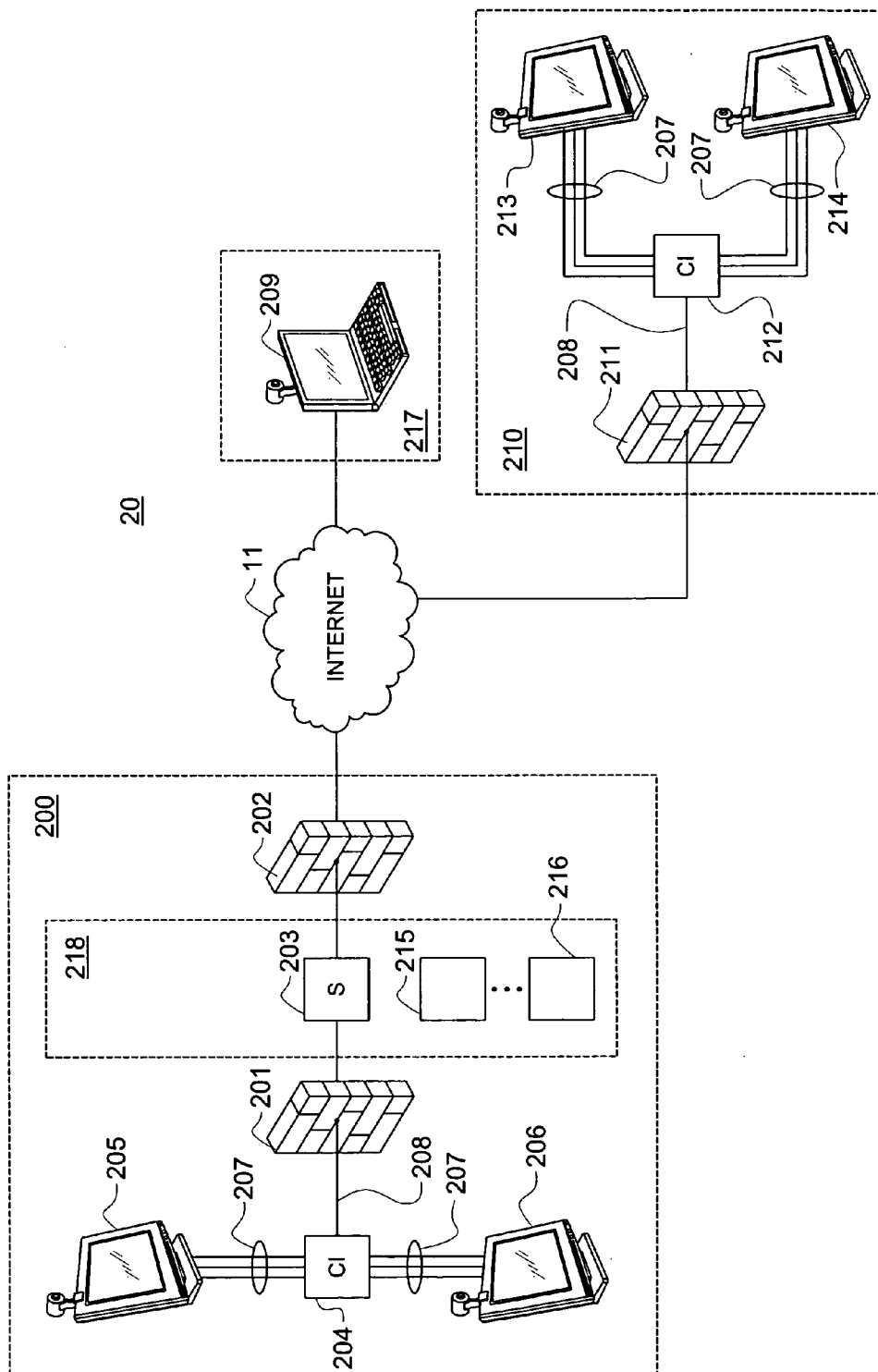


FIG. 4

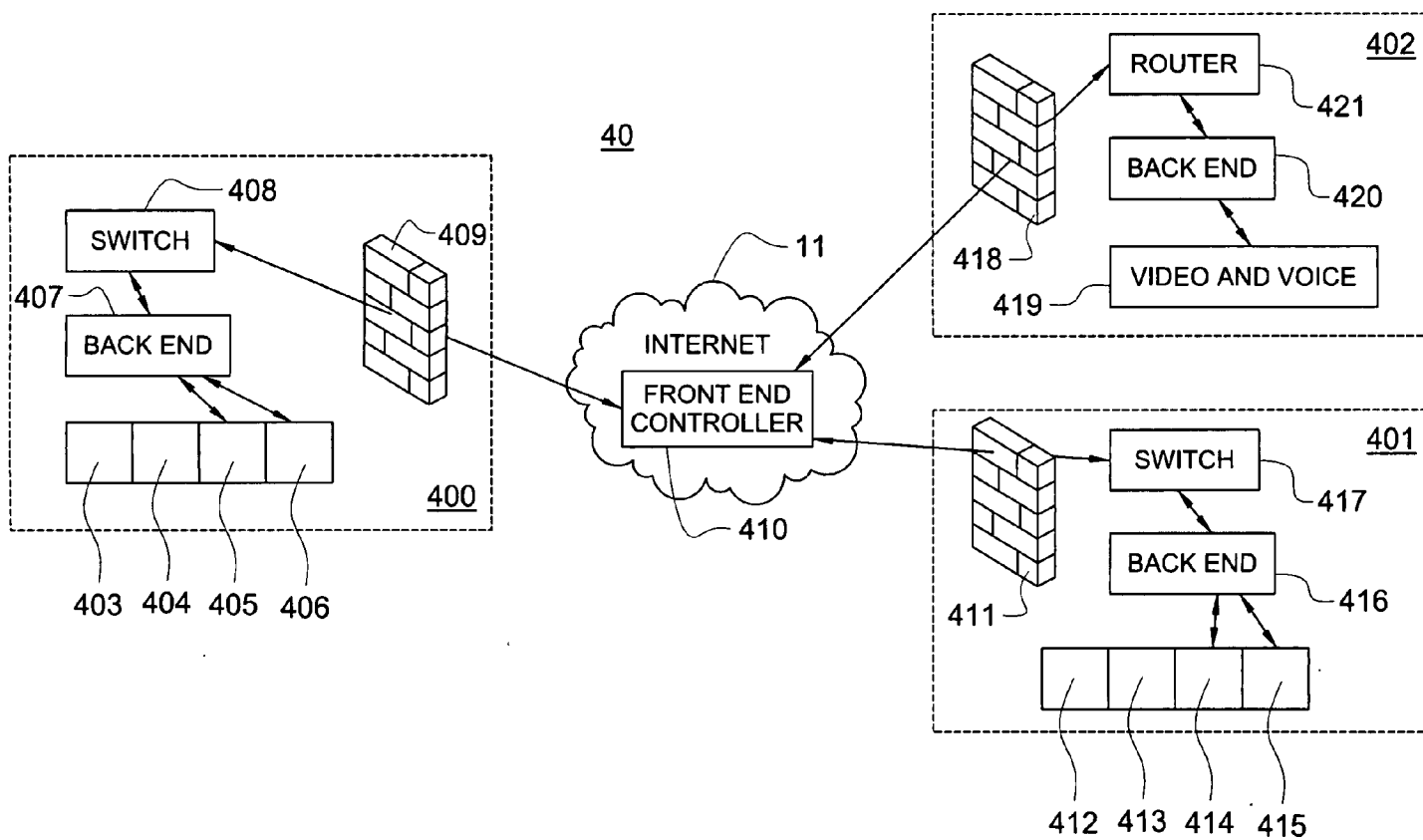


FIG. 5

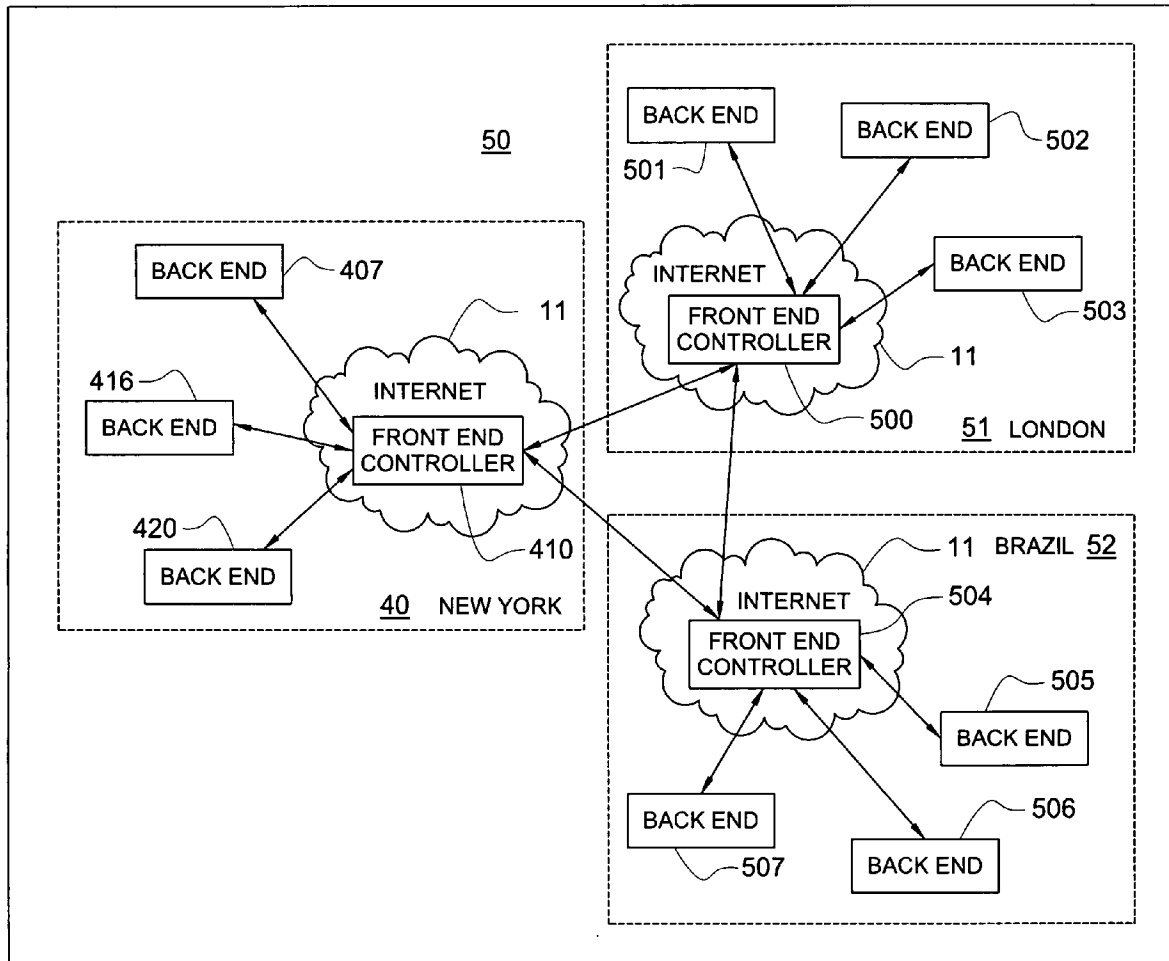
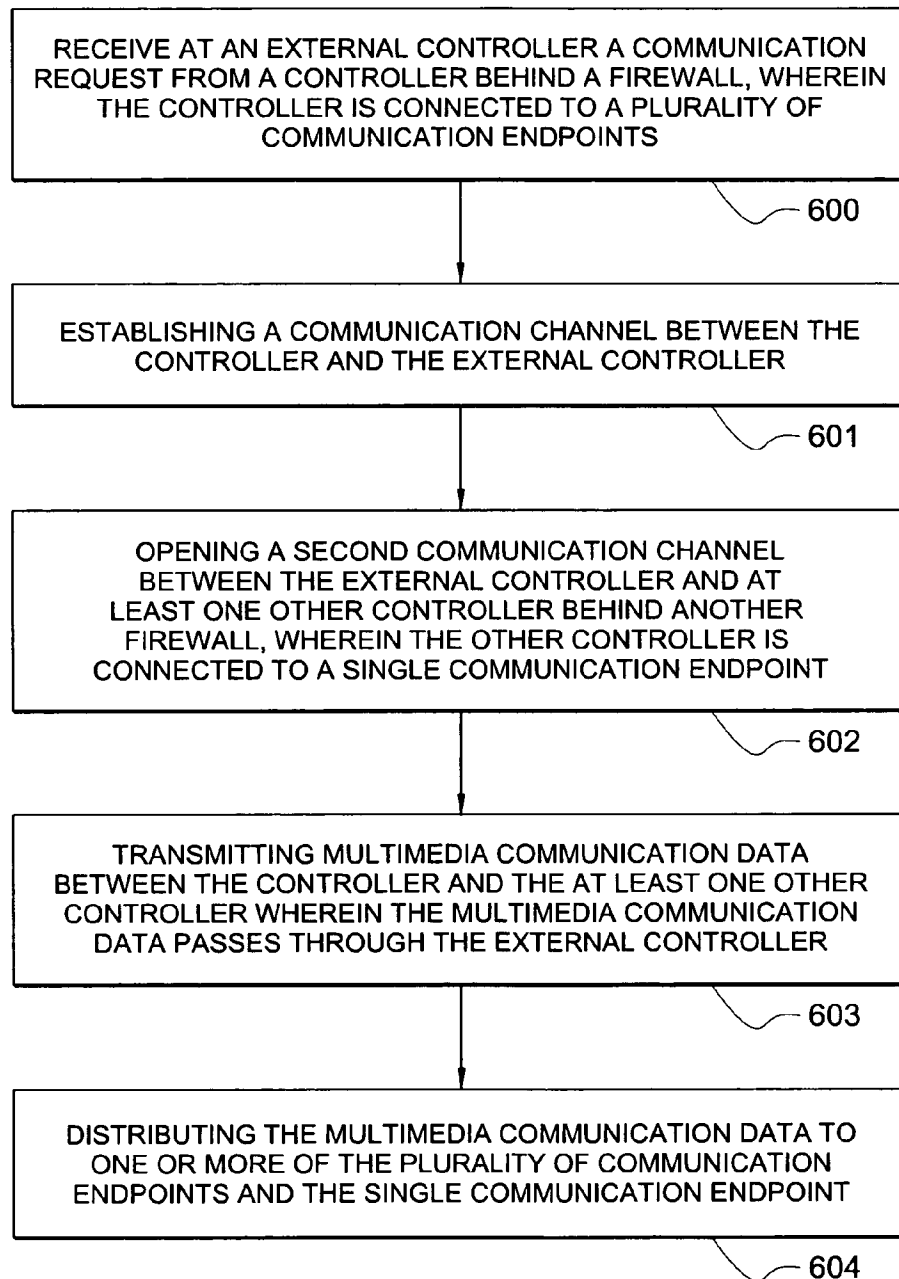


FIG. 6



*FIG. 7*

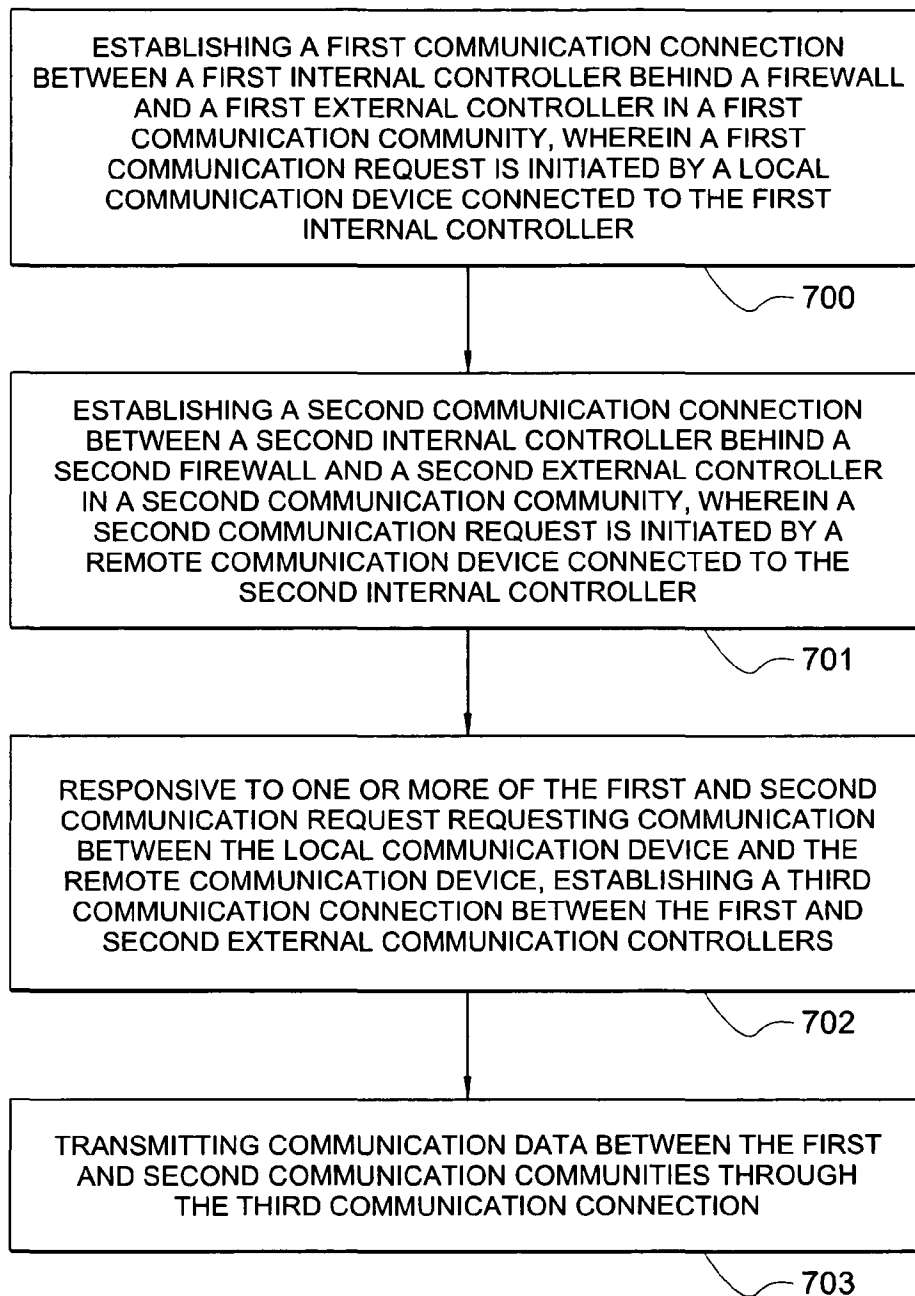


FIG. 8

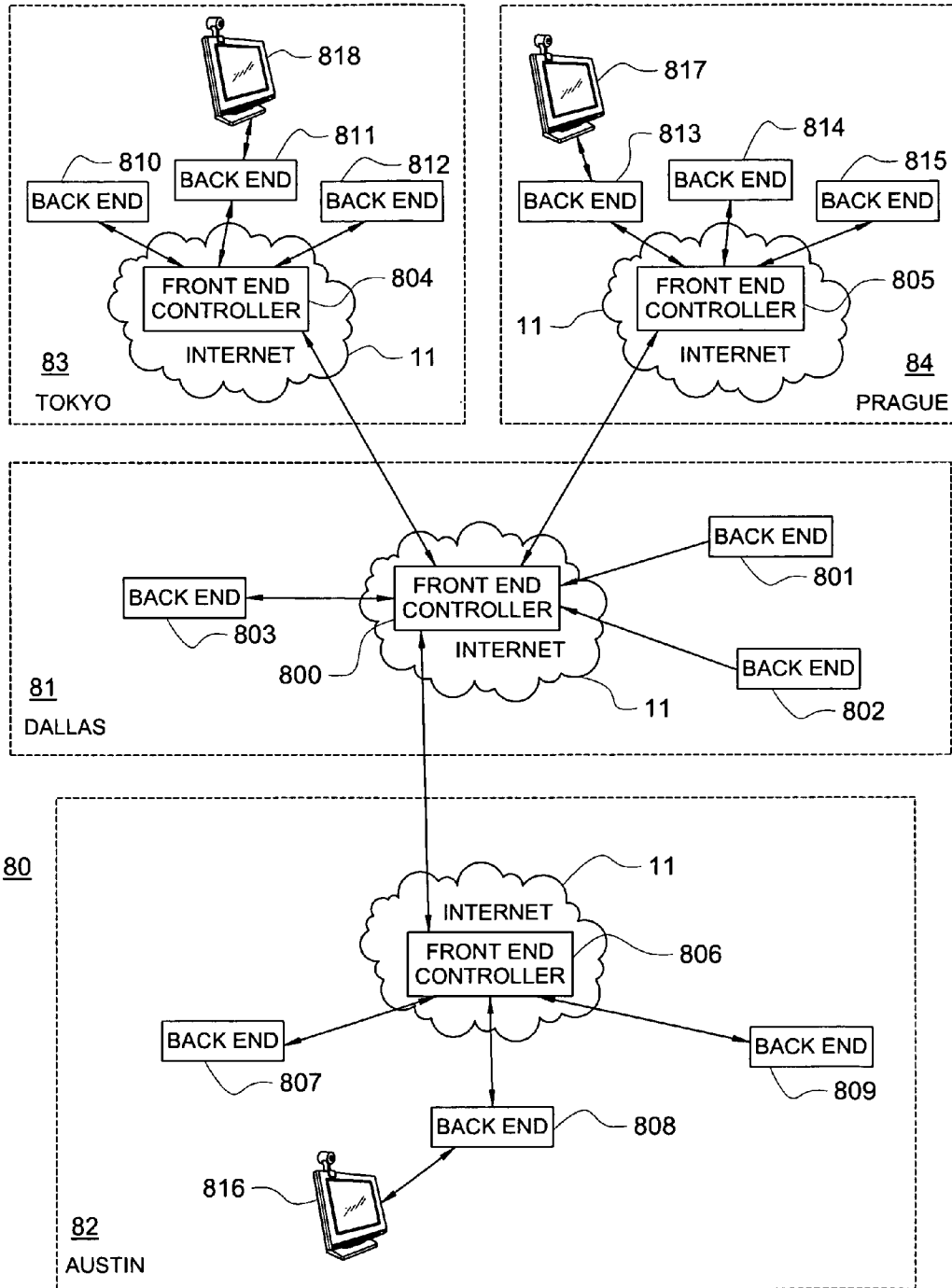
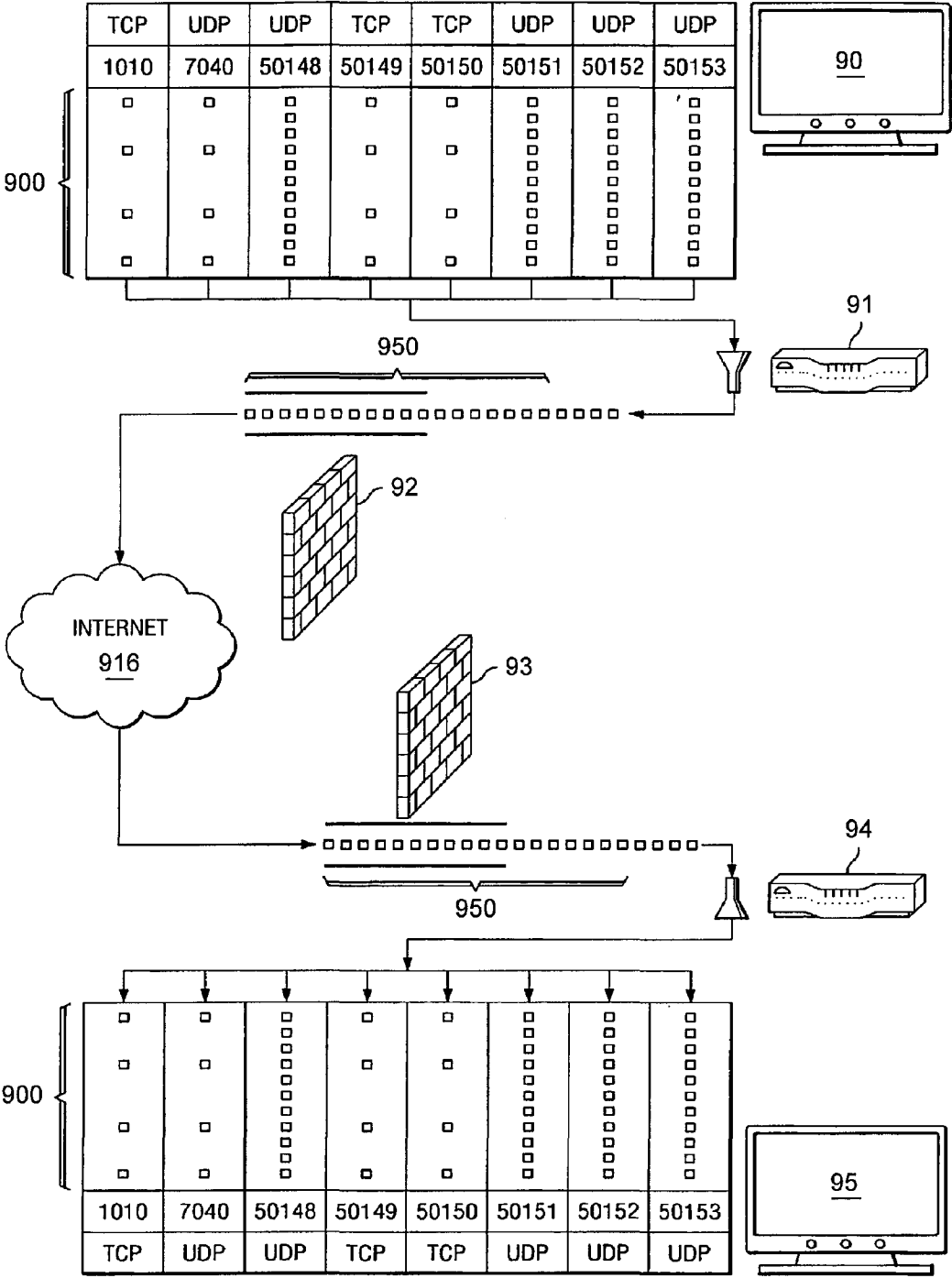
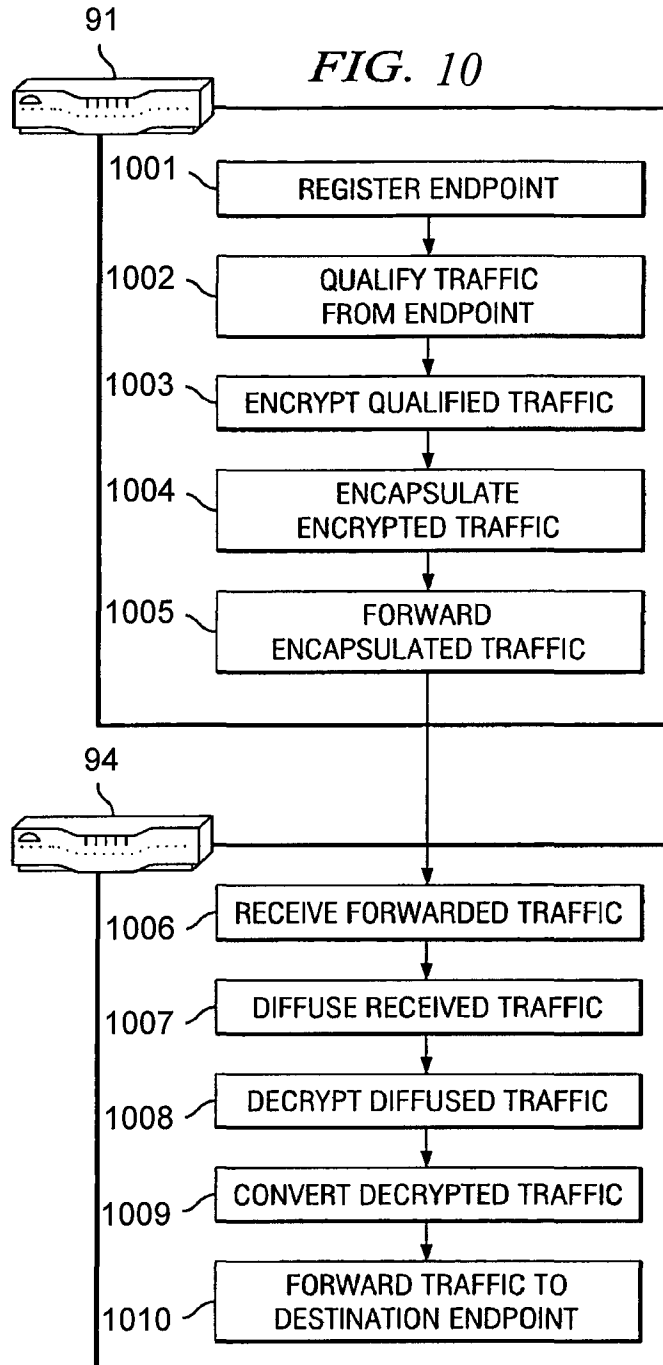




FIG. 9





US 8,560,828 B2

1

## SYSTEM AND METHOD FOR A COMMUNICATION SYSTEM

### CROSS-REFERENCE TO RELATED APPLICATIONS

The present application is related to concurrently filed, co-pending and commonly assigned U.S. patent application Ser. No. 11/403,549, entitled "SYSTEM AND METHOD FOR TRAVERSING A FIREWALL WITH MULTIMEDIA COMMUNICATION," the disclosure of which are hereby incorporated herein by reference.

### TECHNICAL FIELD

The present invention relates, in general, to electronic communications, and, more specifically, to the architecture of a multimedia communication system.

### BACKGROUND OF THE INVENTION

In today's connected electronic society, the technology and know-how to create a completely connected electronic global system has been available and in practice at various levels. However, the utopian ideas of complete and unfettered connectivity are seriously undermined by the electronic "out-laws." Computer viruses, industrial and national spying, information theft, and the like place real dollar risks to maintaining completely free connectivity. Because a genuine need exists for certain computer systems to be connected into the public domain, such as through the public or commodity internet, technology has been developed to provide various levels of protection from computer-based mischief.

One such technology used to minimize the risks for computer-based mischief is a firewall. Firewalls, which can be software, hardware, or a combination of both, are used in modern networks to screen out unwanted or malicious traffic. One of many techniques a firewall may use is packet filtering, wherein the firewall determines whether or not to allow individual packets by analyzing information in the packet header (such as the Internet Protocol (IP) address and port of the source and destination). Thus, various ports (defined below) or IP addresses may be blocked to minimize the risk of allowing malicious traffic into an important computer network or system. Another more advanced technique is called stateful inspection, wherein in addition to analyzing header information, a firewall keeps track of the status of any connection opened by network devices behind the firewall. Deciding whether or not a packet is dropped in a stateful inspection is based on the tracked status of the connection and information from within the packet header. In practice, firewalls (especially those used by large corporations) generally only allow traffic from the well-known ports, though such firewalls may be specially configured to allow traffic on any port. For multimedia communication systems that use multiple registered and dynamic ports, firewalls (unless specially configured) will generally block the data traffic on these ports between multimedia systems, thus, preventing communication.

In communications over the commodity internet, much of the communication occurs using Transmission Control Protocol/Internet Protocol (TCP/IP). TCP/IP is the transport protocol of the internet. One mechanism used to handle IP addresses is the TCP/IP port system. A port is a sixteen bit integer, the value of which falls into one of three ranges: the well-known ports, ranging from 0 through 1023; the registered ports, ranging from 1024 through 49151; and the dynamic and/or private ports, ranging from 49152 through

2

65535. The well-known ports are reserved for assignment by the Internet Corporation for Assigned Names and Numbers (ICANN) for use by applications that communicate using the Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) and generally can only be used by a system/root process or by a program run by a privileged user. The registered ports may be registered for use by companies or other individuals for use by applications that communicate using TCP or UDP. The dynamic or private ports, by definition, cannot be officially registered nor are they assigned.

A TCP/IP port is typically assigned to user sessions and server applications in an IP network. Destination ports are generally used to route packets on a server to the appropriate network application. Thus, some ports are typically associated with particular internet applications. For example, port 80 is the standard port for Hypertext Transport Protocol (HTTP), while port 443 is the standard port for Secure HTTP (HTTPS). HTTP and HTTPS traffic may validly communicate over other ports; however ports 80 and 443 have been assigned as default ports for handling HTTP and HTTPS traffic, respectively. Routers and firewalls typically analyze the port numbers of the incoming data packets to determine how each packet should be handled. Routers review the port number to determine where to route the packet next. When using packet filtering methods, firewalls will review the port numbers to determine whether or not packets from that particular port represent traffic that is known to potentially contain a security threat. If a threat is indicated for that particular port, the packet will be dropped.

Many such firewalls use packet filtering to protect the underlying system. Thus, the ports that typically carry unpredictable packets are usually closed to traffic. In operation, a large number of ports are closed by default. These closed port ranges are usually associated with data traffic for applications that are unpredictable or known to carry undesirable traffic.

Another technique used by some firewalls and many other networking components to interface private or sub-networks with the commodity internet is Network Address Translation (NAT). NAT typically uses a single public IP address for the network interface, but then assigns individual clients on the private or sub-network a dynamic IP address that is selected from a group of private IP addresses for that particular private network or sub-network. NAT has extended the IP address technique beyond its finite number of addresses. However, the translation of addresses becomes a very complicated process when attempting to connect one endpoint to another behind a NAT system.

The use of firewalls and NAT to secure and administer networks has allowed an increase in overall connectivity, while improving the security of those networks. However, with this increased security, adapting to advances in communication technology is hampered. Voice over IP (VoIP) is becoming a popular alternative to the traditional Plain Old Telephone System (POTS) and the Publicly Switched Telephone Network (PSTN). In order to implement VoIP, though, new transmission protocols were developed to handle the specific needs of such system. Session Initiation Protocol (SIP) and H.323 are two examples of such protocols that have been defined for handling the administration of VoIP, and its natural extension to multimedia communication.

H.323 is a multimedia conferencing protocol, which includes voice, video, and data conferencing, for use over packet-switched networks. SIP is a signaling protocol for Internet conferencing, telephony, presence, events notification, and instant messaging. While these protocols allow for

US 8,560,828 B2

3

efficient management of IP-based communication, they run into serious problems when encountering firewalls and NAT systems.

Many communication protocols, including H.323 and SIP, use multiple different ports that can be selected dynamically as the session is initiated. The problem arises because the majority of these ports are closed in typical firewall installations. Therefore, in order to accommodate any type of IP-based communications, large numbers of ports would need to be opened in the firewall. If too many ports remain open, any given entity would risk exposure to potentially harmful unauthorized intrusion.

In NAT systems, each endpoint inside the system does not have a static IP address. Therefore, during setup of point-to-point communication, it is difficult to map out the connection because the target endpoint does not have a fixed, known IP address. The NAT server only provides an IP address when the internal endpoint needs one. Part of the header information in an H.323 or SIP data packet is the destination address. This information may be difficult to know when the NAT server has not assigned an IP address to a specific endpoint or considering that what IP address is assigned for a first call may not be the same IP address assigned for a subsequent call to the same endpoint.

To address this problem of firewall traversal and NAT, companies have designed various solutions from complex systems to simple workarounds. FIG. 1 is a block diagram illustrating a typical complex architecture of IP communication system 10. IP communication system 10 implements a multimedia communication system over the IP protocol. Communication in IP communication system 10 is limited by firewalls 100 and 101. Communication begins with the video and audio captured at endpoint 102. Using a multimedia transport protocol, such as H.323, SIP, or the like, multiple ports are selected by endpoint 102 to effect communication of the multimedia data. Endpoint 102 is connected to gatekeeper 103, which is still behind firewall 100.

Gatekeepers 103 and 107 are special gatekeepers that include proprietary code for establishing a connection over Internet 11 with base controller 106, which is located outside of firewalls 100 and 101. Base controller 106 also includes proprietary code that operates in connection with the code on gatekeepers 103 and 107. In operation, gatekeepers 103 and 107 are registered with base controller 106, such that a known communication setup routine has already been established between them. Firewalls 100 and 101 are modified to open a certain number of specific ports for all communications from gatekeeper 103. The firewall technicians maintaining firewalls 100 and 101 work with the provider of IP communication system 10 on installation to identify the specific ports that communication channels 105 will be transmitted over. Once those ports are opened, IP communication may occur over channels 105.

Gatekeepers 103 and 107 also provide for converting communication streams that may originate for different ports into channels 105. For example, monitor 102 communicates using H.323 which uses communication channels 104. Gatekeeper 103 shifts the data from communication channels 104 over to communication channels 105 in order to traverse firewall 100.

IP communication system 10 may also include special communication equipment, such as communication unit 109, which includes special proprietary code specifically developed for use in IP communication system 10. When using this special equipment, a user is able to connect to base controller 106 without first connecting to gatekeeper 103. Communication unit 109 is also registered with base controller 106 and packages all communication streams into channels 105 to

4

traverse firewall 100 using the specified ports. Thus, a user at communication unit 109 may establish IP communication with a user at endpoint 108 without first connecting to gatekeeper 103. Examples of such systems configured similar to IP communication system 10 are provided by companies such as TANDBERG and the like. The limitation of such systems is that holes are still opened in the firewalls. There is nothing already in the security provisions of the firewalls that would prevent hostile traffic from entering through the ports that are opened to implement IP communication system 10.

FIG. 2 is a block diagram illustrating IP communication system 20. IP communication system 20 is configured to allow various levels of IP communication between individuals located at entity site 200, remote entity site 210, and home site 217. IP communication system 20 is implemented using a base server, communication server 203, in communication with individual client instances, clients 204, 209, and 212. At entity site 200, communication server 203 is placed in the middle-network zone, DMZ 218, which is the sub-network that sits between the trusted network of entity site 200 and Internet 11. Many network components or servers that have direct connectability to Internet 11 are situated within DMZ 218. For example, in addition to communication server 203, DMZ 218 also contains e-mail server 215, Web server 216, and the like. DMZ 218 is typically delimited by the private network firewall, such as private firewall 201, and an Internet firewall, such as Internet firewall 202. Internet firewall 202 maintains more open ports that are typically useful in receiving Internet-driven communication, such as email, Web-requests, and the like, while private firewall 201 is much more restrictive in the ports that it allows to have access into the private network of entity site 200.

When IP communication is desired, endpoints 205 and 206 each establish connections to client 204. Client 204 receives all of the communication streams directed to different ports, multi-port communications 207, and multiplexes those different communication streams into a single stream directed to a single port, single port data stream 208. In setting up IP communication system 20, the firewall administrators designate a single, specific port in both private firewall 201 and Internet firewall 202 for accepting data packets. Client 204 then transmits the multiplexed communication over single port data stream 208 to communication server 203 via private firewall 201. Communication server 203 will then transmit the multiplexed communication to the targeted endpoint at either one or both of remote entity site 210 and home site 217. Similarly, endpoints 213 and 214 communicate with client 212, which multiplexes the communications on multi-port communications 207 into a single port stream on single port data stream 208. Client 212 then transmits the multiplexed communication stream through remote firewall 211 and Internet firewall 202 to communication server 203. The communication stream from client 212 comes into Internet firewall 202 addressed to the specific port designated for the IP communication. Internet firewall 202, therefore, lets the data packets through to communication server 203. Communication server 203 is then able to transmit the communication stream to client 204 through private firewall 201.

FIG. 3 is a block diagram illustrating IP communication system 30. Instead of opening up new holes in firewalls 300 and 301, or using any existing open ports, IP communication system 30 simply goes around the company firewall, e.g., firewalls 300 and 301. IP communication system 30 connects to Internet 11 using a standard, non-secure Internet connection, connection 304. IP communication system 20 comprises endpoints 302 and 303 that include proprietary code enabling IP communication to be established over connection 304.

US 8,560,828 B2

5

Because neither connection **304** nor the communication equipment (i.e., endpoints **302** and **303**) are connected into the users systems, there is little danger that any faults or malevolent traffic will jeopardize the system. However, implementing a totally separate system does not take advantage of the benefits that can be attributed to using the entity's protected, backend system. An example of such a system that addresses the firewall and NAT problem by completely bypassing the company's protected, backend system are video conferencing systems from Polycom, Inc.

#### BRIEF SUMMARY OF THE INVENTION

The present invention is directed to a system and method for managing a communication system. The system is made up of several communication communities that provide communication between each of the various endpoints connected into the community and also allows for the individual communities to inter-communicate with the other communities in the communication network. In establishing the communication configuration in one of the communities/sub-communities, a communication request is received at an external controller from a first controller behind a firewall. The first controller connects to multiple endpoints provided for users. A communication channel is established between the first controller and the external controller after the external controller has authenticated or verified the identification of the first controller. A second communication channel is opened between the external controller and at least one other controller behind another firewall, where the other controller is connected to a single communication endpoint. In the configuration of the community/sub-community in selected embodiments of the present invention, then, there is at least one controller that services multiple endpoints and at least one other controller that is dedicated for a single endpoint. Multimedia communication data is transmitted between the first controller and the other controller where the multimedia communication data is distributed to the communication endpoints, including the single communication endpoint, that are connected to or participating in the particular communication session.

The various additional representative embodiments of the present invention also include inter-communication between the communities/sub-communities described above. Communication in the first community is established as described above: the endpoint requests communication from the internal controller, which makes that request outside of the firewall to the external controller. Communication in any other communication community is also established similarly. Another endpoint requests communication to the internal controller that it is connected to, which then makes that request outside of its firewall to the other external controller. Once everything is verified, a communication channel is open between the other endpoint and the other external controller. When either of the communication requests request communication between endpoints located in the separate communities, another communication connection is established between the two external communication controllers of the different communities. The communication data would then be transmitted between the two controllers through that connection.

The foregoing has outlined rather broadly the features and technical advantages of the present invention in order that the detailed description of the invention that follows may be better understood. Additional features and advantages of the invention will be described hereinafter which form the sub-

6

ject of the claims of the invention. It should be appreciated by those skilled in the art that the conception and specific embodiment disclosed may be readily utilized as a basis for modifying or designing other structures for carrying out the same purposes of the present invention. It should also be realized by those skilled in the art that such equivalent constructions do not depart from the spirit and scope of the invention as set forth in the appended claims. The novel features which are believed to be characteristic of the invention, both as to its organization and method of operation, together with further objects and advantages will be better understood from the following description when considered in connection with the accompanying figures. It is to be expressly understood, however, that each of the figures is provided for the purpose of illustration and description only and is not intended as a definition of the limits of the present invention.

#### BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present invention, reference is now made to the following descriptions taken in conjunction with the accompanying drawing, in which:

FIG. 1 is a block diagram illustrating a typical complex architecture of an IP communication system;

FIG. 2 is a block diagram illustrating another IP communication system;

FIG. 3 is a block diagram illustrating another IP communication system;

FIG. 4 is a block diagram illustrating a communication community configured according to one embodiment of the present invention;

FIG. 5 is a block diagram illustrating an extended communication community configured according to one embodiment of the present invention;

FIG. 6 is a flowchart illustrating example steps executed in implementing one embodiment of the present invention;

FIG. 7 is a flowchart illustrating example steps executed in implementing one embodiment of the present invention; and

FIG. 8 is a block diagram illustrating a communication environment configured according to one embodiment of the present invention.

FIG. 9 is a diagram illustrating an IP communication system configured according to one embodiment of the present invention; and

FIG. 10 is a flowchart showing for an embodiment of the invention, example steps that may be employed to traverse a firewall.

#### DETAILED DESCRIPTION OF THE INVENTION

FIG. 4 is a block diagram illustrating communication community **40** configured according to one embodiment of the present invention. Communication community **40** establishes a reliable multimedia communication system between multiple locations and multiple users at those different locations. For purposes of this example, principal office **400** is the principal business location for a company. Satellite office **401** is a branch office located in a suburb of the city where principal office **400** is located. Travel office **402** is a hotel room across the country where the company's CEO is attending a company meeting. Communication community **40** allows the company CEO to establish connection into the community from where ever he is located and has access to Internet **11**.

The features of communication community **40** are implemented by the system architecture operating at each location.

US 8,560,828 B2

7

Principal office **400** includes multiple endpoints, **403-406**, such as telephones, computer terminals, and the like, that are configured for multimedia communication. Each of multiple endpoints **403-406** is connected to backend controller **407**. Backend controller **407** manages the communication interactions with endpoints **403-406** and allows the communication to be transmitted to switch **408** and firewall **409** and eventually out to Internet **11** and front end controller **410**.

In setting up the components of communication community **40**, each of the components is registered with the other. For example, each of backend controllers **407** and **416** registers with front end controller **410**. This process may be performed during initial system setup by Information Technology (IT) professionals. Backend **420** is also registered with front end controller **410**. However, because backend **420** is a portable unit, once registered, various individuals may use backend **420** to establish verified connections into communication community **40** from remote, temporary locations. Again, the registration procedure for backend **420** may also be performed by IT professionals. Each endpoint, endpoints **403-406**, **412-415**, and **419** may also register with their associated backend controller. By registering each component to communication community **40**, communication may be more-reliably established because each component is aware of the detailed identification information of the other components in the system.

It should be noted that back end controller **407** may be configured according to various multimedia communication protocols and systems. One example of such a system is described in technology covered by co-pending, commonly owned, U.S. patent application Ser. No. 11/403,549, entitled, "SYSTEM AND METHOD FOR TRAVERSING A FIREWALL WITH MULTIMEDIA COMMUNICATION." Such technology converts multiport transport protocols, such as H.323, SIP, and the like, into a single port transport protocol that can easily traverse firewalls with valid, standard single-port traffic.

A variety of protocols require the use of multiport traffic. Whether the traffic is data between applications, voice communications, or video conferencing, whenever multiport traffic is used there is a possibility of some or all of the traffic being blocked by a firewall between two devices that are attempting to communicate. As an example, video conferencing systems, whether they are based on H.323, SIP, or other similar multimedia communication protocols, use multiple ports and multiple protocols in order to enable two-way audio and video communication. The communication protocols specify different types of traffic that may be sent between endpoints which include media traffic (voice, video, and the like) along with the control traffic (camera, connection control, and the like). The media traffic is comprised of data for the images and sound being transmitted between endpoints with the control traffic comprising data used to control the connection between endpoints and the features of the endpoint (e.g., camera direction, zoom, and the like). Due to its higher throughput rate, UDP may typically be utilized for the real-time communication traffic between endpoints. TCP may be utilized for traffic requiring data integrity (e.g., control traffic). As such, video conferencing systems typically make use of both TCP and UDP to transport the multimedia data to enable communication. The ports that are typically used to enable the two-way communication include various ports across the well-known ports, the registered ports, and the dynamic ports. Firewalls are usually set up to block unrequested traffic and/or traffic coming in on dynamic ports. Furthermore, UDP does not provide a mechanism for identifying received traffic as requested traffic. Thus, programs and

8

endpoints that send traffic conforming to UDP are at risk of having that traffic blocked by the remote endpoint's firewall for both being unrequested and being sent on a blocked port.

Referring to FIG. 9, video conference endpoint **90** attempts to send multimedia data (packets **900**) to video conference endpoint **95**, with network devices (e.g., backend controllers) **91** and **94** in the system. In this embodiment, endpoint **90** is a video conference endpoint that uses a multiple port communication protocol in order to establish communication with endpoint **95**. For the purposes of this example, endpoint **90** uses ports 1010, 7030, 50148-50153. The data transmitted using ports 1010 and 50149-50150 utilize TCP as the transport protocol while the data transmitted using ports 7030, 50148, and 50151-50153 utilize UDP as the transport protocol. Packets from each of these ports conforming to these various protocols and sub-protocols are received by network device **91**. It should be noted that additional or alternative examples of endpoints may use more or fewer ports of different numbers based in part on the applications or protocols used to facilitate multimedia communication.

The received packets are encapsulated to conform to a protocol used by devices **91** and **94** for transmitting data, which may include, but is not limited to: TCP, UDP, Stream Control Transmission Protocol (SCTP), Datagram Congestion Control Protocol (DCCP), Real-time Transport Protocol (RTP), and the like. Device **91** receives packets **900** from endpoint **90** that conform to both TCP and UDP, encapsulates each of multiport packets **900** into single-port packets **950** that conform to a single-port communication protocol used by devices **91** and **94**, and sends packets **950** to device **94**. The method of encapsulation may comprise using some or all of the information (header and data) within each of packets **900** as the data section for encapsulated packets **950**.

The encapsulated packets are sent to device **94** using any of the well-known or registered ports, which are the ports that are typically open in standard firewalls. One such well-known port that could be chosen is port 443, which is commonly reserved for HTTPS traffic by ICANN and is commonly open by default on most firewalls. While the packets may be sent along any of the well-known, registered, or dynamic ports, the preferable port used may be a port that is commonly open on most firewalls in their standard configurations (e.g., the well-known ports, certain registered ports, and the like).

Firewall **92** inspects the traffic from device **91** before sending it out through Internet **916** to device **94**. When the traffic arrives at firewall **93**, it inspects the traffic, determines that it is valid traffic on a well-known port, and passes it along to device **94**.

Device **94** receives encapsulated single-port packets **950** sent from device **91**. Device **94** then reconstructs multiport packets **900** using packets **950**. Reconstruction may be performed by any suitable method including hash-like functions or tables. As an example, header information within one of packets **950** may be an input to a hash-like function that returns the destination IP address and port numbers for a given packet. In the case of a hash-like table, device **91** may use a portion of the header or data in each of packets **900** as the index of a hash-like table and then convert packets **900** to packets **950**. Device **94** upon receiving packets **950**, may use a portion of the header or data in each of packets **950** as the index of a hash-like table and then reconvert packets **950** back to packets **900**, recovering the original IP addresses and ports based on information stored in the hash-like table.

From the original headers, device **94** determines for each packet that it is for delivery to endpoint **95**. Device **94** then sends the packets to endpoint **95** using each packet's destination port. Thus, if a port and protocol are advantageously

US 8,560,828 B2

9

chosen (such as port 443 and Secure Sockets Layer (SSL)), communications traffic from endpoint **90** may be sent to endpoint **95** with no modification or user intervention to traverse firewalls **92** and **93**. While one-way communication is described (from endpoint **90** to endpoint **95**) it is noted that each of devices **91** and **94** may perform the steps of receiving multiple packets, encapsulation, port translation, decapsulation, and resending multiple packets in order to enable two-way communication between endpoints **90** and **95**. Additional or alternative embodiments may use any of the well-known or registered ports that are typically or commonly open in standard firewalls to send packets between devices **91** and **94**. While any of the well-known, registered, or dynamic ports may be used, it is preferable to select a port that is commonly open in firewalls.

It should be noted that in additional or alternative embodiments of the present invention, network or other errors may occasionally lead to lost or corrupted packets and some protocols (such as TCP) specify that in such cases these lost or corrupted packets be resent, which is at odds with maintaining real-time communication. With real-time communication, current data takes precedence over lost previous data since resent packets of previously lost or corrupt data may arrive too late to be useful. As such, when receiving a request to resend a packet containing real-time data (e.g. data corresponding to the audio or video of the communication) devices **91** and **94** may simply ignore the resend request or, alternatively, send a current data packet masquerading as the previously sent and subsequently lost packet, as alternate data.

FIG. **10** is a flowchart that shows for an embodiment of the invention, example steps that may be employed by devices **91** and **94** to traverse a firewall. An endpoint, when connected to a network, first registers with device **91** by the endpoint identifying itself as a compliant endpoint (e.g., it is an endpoint that conforms to H.323, SIP, VoIP, or the like), as shown by step **1001**.

On a given network, multiple devices may be connected, as such, device **91** may receive traffic from many devices within that network. Thus, device **91** qualifies the traffic it receives to ensure that the traffic sent to device **94** is appropriate traffic. This is shown in step **1002** and may be accomplished by comparing a given packet's source IP and port addresses to those of endpoints that have registered with device **91**. In step **1003**, device **91** encrypts the previously qualified traffic securing the communication between two endpoints using any suitable encryption method including, but limited to: AES 128-bit, TDES, Skipjack, or the like. In step **1004**, the encrypted traffic is then encapsulated to conform to a single port protocol, such as SSL, by placing the previously encrypted packet into a new packet conforming to SSL protocol. As shown by step **1005**, the encapsulated traffic is then forwarded to device **94**.

In step **1006**, device **94** receives the single port traffic from device **91** and is diffused by step **1007** by restoring the original IP addresses and port numbers to the individual packets. In step **1008**, this diffused traffic is then decrypted, thus, recovering the original multimedia and control communication information within the packets. In step **1009**, the packets are then restored to their original transport protocol, such as TCP, UDP, or the like. With the packets being fully restored, they are then forwarded to the destination endpoint by device **94**, as shown by step **1010**.

It is noted that while the disclosure has used the communication between two video conference endpoints as an example, it is understood that the systems and methods described may be used by other programs, applications, communications systems, and the like, that use multiport proto-

10

cols for communication. As such, embodiments of the invention may be used for audio systems VoIP systems, or any other system that uses a multiport protocol to transfer data between devices. Referring back to FIG. **9** as an example, endpoints **90** and **95** may be VoIP endpoints engaging in voice communication. In this embodiment the multiport VoIP protocol traffic from endpoint **90** may be received by device **91**, converted to a single port protocol by device **91**, encapsulated by device **91**, transmitted to device **94**, decapsulated by device **94**, converted back to the original multiport protocol by device **94**, transmitted to endpoint **95**, and received by endpoint **95**, as described in further detail above. The same holds true for other types of programs, equipment, or applications using a multiport protocol to transfer data across a network.

Front end controller **410** is located outside of firewall **409**. It has an address, which can be an IP address, a Uniform Resource Locator (URL), or the like, that is known specifically by back end **407**. Moreover, front end controller **410** maintains a security table that allows it to selectively connect with only those backend controllers that have a valid security key. For example, endpoint **406** desires to make a video call to another party within communication community **40**. Backend controller **407** knows the address for front end controller **410**. In order to initiate the communication, backend controller **407** transmits a request through switch **408** and firewall **409** to the specific address of front end controller **410** for such communication. Along with the request, backend controller **407** also sends a security key. When front end controller **410** receives the request and the key, it first verifies and authenticates the key to make sure that the component requesting access is a valid and authorized component. Once it is authenticated as a valid backend, the request for communication is opened and the multimedia communication stream will be managed by front end controller **410** between endpoint **406** and its destination address.

Each of the other locations in communication community **40** has similar configurations as principal location **400**. Satellite location **401** includes endpoints **412-415**, backend controller **416**, switch **417**, and firewall **411**. Travel office **402** includes a single endpoint, endpoint **419**, backend controller **420**, and router **421**, which may be the high speed modem found in the CEO's hotel room. The hotel Internet system also provides firewall **418**. The configuration of communication community **40** that joins each of principal office **400**, satellite office **401**, and travel office **402** provides a unique communication system architecture. The key components of this system of communication community **40** include the backends located behind each firewall, backend controllers **407**, **416**, and **420**, where backend **420** provides only for a single endpoint connection; front end controller **410**, which facilitates the communication by providing a known component outside of the firewalls that has a known connection pipe to each of backend controllers **407**, **416**, and **420**; and endpoints **403-406**, **412-415**, and **419**, which provide the multimedia communication devices for the communication. By providing these components both in front of and behind the various firewalls, communication community **40** provides a robust, secure, and highly scalable communication system.

It should be noted that in various additional or alternative embodiments of the present invention, each location other than travel office **402** could have different numbers of endpoints connected thereto depending on the capacity of the associated backend controller. Moreover, each location may be separated by any distance, as long as the endpoints or backends can access Internet **11**. Such access may be accommodated through wired connections or wireless connections to any of the points within the system.

US 8,560,828 B2

11

FIG. 5 is a block diagram illustrating expanded communication community (ECC) 50 configured according to one embodiment of the present invention. ECC 50 creates a scaled communication network by combining or joining the communication capabilities of several communication sub-systems into a single expanded community. For example, communication community 40, as described in FIG. 4, is noted in ECC 50 as being located in New York. It is joined with communication community 51 and 52 located in London and Brazil, respectively. Each member state (i.e., communication communities 40, 51, and 52) of ECC 50 is at once an autonomous communication system and a shared communication system facilitating multimedia communication between endpoints in Brazil, London, and New York. The association of backend controllers 407, 416, and 420 with front end controller 410 facilitates communication in New York, while the association of backend controllers 501-503 with front end controller 500 facilitates communication in London, and the association of backend controllers 505-507 with front end controller 504 facilitates communication in Brazil.

When a user with an endpoint connected to backend controller 416 desires to participate in multimedia communication, such as a video conference, with a user with an endpoint connected to backend controller 503 in London, backend controller 416 requests to initiate communication with front end controller 410 with the identification information from the New York user's endpoint. After verifying and authenticating the security key transmitted over Internet 11 by backend controller 416, front end controller 410 opens a communication channel between itself and backend controller 416. The communication request information from the New York endpoint transmitted by backend controller 416 to front end 410 includes the destination address of the London endpoint. Front end 410 recognizes that the destination endpoint does not reside within its communication community 40. Using a communication table stored with front end controller 410, front end controller 410 looks up the address to initiate communications with the London endpoint. Front end controller transmits a communication request to front end 500 within communication community 51 that includes a security key and other identification information.

Upon receipt of the communication request from front end controller 410, front end controller 500 verifies and authenticates the security key just as it would when receiving a communication request from any of backend controllers 501-503. In fact, when any of front end controllers 410, 500, and 504 receive communication requests from any other front end controller, it views that request as being from any other backend controller. The front end controllers make no distinction between communication from front end controllers or backend controllers.

When front end controller 500 authenticates and verifies the communication request from front end controller 410, a communication path is opened between the two. Front end controller 500 also will use the address of the London endpoint to establish communication with backend controller 503 and then, subsequently, with the destination endpoint. Once the communication lines have been established between the New York and London endpoints, the New York and London users may communicate using multimedia data, such as with video, audio, and data.

FIG. 6 is a flowchart illustrating example steps executed to implement one embodiment of the present invention. In step 600, a communication request is received at an external controller from a first controller behind a firewall, where the controller is connected to a plurality of communication endpoints. A communication channel is established, in step 601,

12

between the controller and the external controller. A second communication channel is opened, in step 602, between the external controller and at least one other controller behind another firewall, where the other controller is connected to a single communication endpoint. In step 603, multimedia communication data is transmitted between the first controller and the other controller where the multimedia data passes through the external controller. The multimedia communication data is distributed, in step 604, to the selected communication endpoints including the single communication endpoint.

FIG. 7 is a flowchart illustrating example steps executed to implement one embodiment of the present invention. In step 700, a first communication connection is established between a first internal controller behind a firewall and a first external controller in a first communication community, where a local communication device connected to the first internal controller initiates a first communication request. A second communication connection is established, in step 701, between a second internal controller behind a second firewall and a second external controller in a second communication community, where a remote communication device connected to the second internal controller initiates a second communication request. In response to either communication request requesting communication between the local and remote communication devices, a third communication connection is established, in step 703, between the first and second external communication controllers. In step 704, communication data is transmitted between the first and second communication communities through the third communication connection.

FIG. 8 is a block diagram illustrating communication environment 80 configured according to one embodiment of the present invention. Communication environment 80 is made up of several sub-communities: Dallas communication community (DCC) 81, Austin communication community (ACC) 82, Tokyo communication community (TCC) 83, and Prague communication community (PCC) 84. As with ECC 50, described in FIG. 5, each of the different sub-communities is capable of acting as its own autonomous communication community. However, the embodiment described in FIG. 8 includes a hierarchical relationship amount the various communities and, more specifically, the front end controllers.

The front end controller for DCC 81, front end controller 800, is configured to be a super controller. A super controller, as contemplated and described for the embodiment described in FIG. 8, is the main front end controller and operates as the communication conduit for the other sub-communities. While front end controller 800 facilitates data transfer between the backend controllers within DCC 81, backend controllers 801-803, it also facilitates data transfer between the backend controllers of ACC 82, backend controllers 807-809; TCC 83, backend controllers 810-812; and PCC 84, backend controllers 813-815.

In operation, a user at endpoint 816 desires to enter a video conference. The connection at endpoint 816 requesting to enter into the video conference causes backend controller 808 to transmit a communication request to front end controller 806 over Internet 11. Users at endpoint 818, in Tokyo, and endpoint 817, in Prague, also desire to participate in the video conference. The video conference requests from endpoint 817 and 818 cause backend controllers 813 and 811, respectively, to transmit communication requests to front end controllers 805 and 804, respectively. After authenticating and verifying the security keys transmitted by each of backend controllers 808, 811, and 813, front end controllers 804-806 open communication channels within ACC 82, TCC 83, and PCC 84. However, because the users within the different



US 8,560,828 B2

13

sub-communities are to be on the same video conference, the video data will be shared across the community borders of ACC 32, TCC 83, and PCC 84.

Instead of each sub-community communicating directly with the other sub-communities, as reflected in the embodiment described in FIG. 5, front end controllers 804-806 transmit the multimedia data to each other through the super controller, front end controller 800. Each of front end controllers 804-806 is configured to establish a communication connection with front end controller 800 whenever a destination address is located outside of its sub-community. Thus, once the communication channel is open in TCC 83 between endpoint 818 and front end controller 804, front end controller 804 transmits a communication request to front end controller 800. Front end controller 800 verifies and authenticates the security key transmitted from front end controller 804 and, once verified, the communication channel is opened. Front end controller 800 uses destination information for the video conference to open communication channels between itself and front end controller 805, to facilitate delivery and receipt of the video conference data to endpoint 817 in PCC 84, and front end controller 806, to facilitate delivery and receipt of the video conference data to endpoint 816 in ACC 82. A similar process is used when communication channels are to be set up between front end controllers 805 and 806 and front end controller 800.

It should be noted that in various additional and alternative embodiments of the present invention, the super controller, front end controller 800 may be configured to receive data and open communications channels only with specific network elements, such as with backend controllers 801-803 and front end controllers 804-806. By limiting the authorized network elements that may contact the super controller, the risk of unauthorized access to communication environment 80 is diminished.

It should be noted that in additional and/or alternative embodiments of the present invention, all front end controllers may be configured to communicate with specific network devices. As noted above, limiting the pool of potential devices that may access any particular front end controller, greatly reduces the risk of unauthorized access.

Although the present invention and its advantages have been described in detail, it should be understood that various changes, substitutions and alterations can be made herein without departing from the spirit and scope of the invention as defined by the appended claims. Moreover, the scope of the present application is not intended to be limited to the particular embodiments of the process, machine, manufacture, composition of matter, means, methods and steps described in the specification. As one of ordinary skill in the art will readily appreciate from the disclosure of the present invention, processes, machines, manufacture, compositions of matter, means, methods, or steps, presently existing or later to be developed that perform substantially the same function or achieve substantially the same result as the corresponding embodiments described herein may be utilized according to the present invention. Accordingly, the appended claims are intended to include within their scope such processes, machines, manufacture, compositions of matter, means, methods, or steps.

What is claimed is:

1. A method for a multimedia communication comprising: receiving, at a controller that is behind a firewall and that is communicatively coupled with a plurality of endpoint communication devices, a plurality of multiport packets

14

of data in a multiport communication protocol for communication from at least one of the plurality of endpoint communication devices;

converting, by said controller, said plurality of multiport packets into a plurality of single-port packets in a single-port communication protocol;

receiving at an external controller a communication request from said controller behind said firewall, wherein said external controller is not behind said firewall;

establishing a communication channel between said controller and said external controller;

opening a second communication channel between said external controller and at least one other controller behind another firewall, wherein said at least one other controller is configured to service a single endpoint communication device;

transmitting multimedia communication data between said controller and said at least one other controller wherein said multimedia communication data passes through said external controller; and

distributing said multimedia communication data to one or more of said plurality of endpoint communication devices and said single endpoint communication device.

2. The method of claim 1 further comprising:

verifying said communication request at said external controller.

3. The method of claim 1 further comprising:

transmitting a security key from said controller to said external controller for authorization of said communication request.

4. The method of claim 1 further comprising:

sending an external request from said external controller to an additional external controller responsive to said communication request requesting to communicate with an additional endpoint communication device connected to said additional external controller.

5. The method of claim 4 further comprising:

establishing an external channel between said external controller and said additional external controller; and forwarding said multimedia communication data to said additional external controller from said external controller; and

distributing said multimedia communication data to said additional endpoint communication device.

6. The method of claim 1 further comprising:

issuing a central request from said external controller to a central controller responsive to said communication request requesting to communicate with an external endpoint device not connected to one or more of said controller and said at least one other controller; and receiving said multimedia communication data at said central controller.

7. The method of claim 6 further comprising:

determining a peripheral controller connected to said external endpoint device;

opening another external channel between said central controller and said peripheral controller;

forwarding said multimedia communication data to said peripheral controller from said central controller; and distributing said multimedia communication data to said external endpoint device.

8. The method of claim 6 further comprising:

distributing said multimedia communication data to said external endpoint device when said external endpoint device is connected to said central controller.

US 8,560,828 B2

15

9. The method of claim 1 wherein said transmitting said multimedia communication data between said controller and said at least one other controller comprises:

transmitting from said controller said plurality of single-port packets over a commonly-open port to said at least one other controller, said plurality of single-port packets traversing one or more firewalls using said commonly-open port.

10. The method of claim 9 further comprising:

receiving said plurality of single-port packets at said at least one other controller;

reconverting, by said at least one other controller, said received plurality of single-port packets into said multiport communication protocol, resulting in reconverted plurality of multiport packets; and

delivering, from said at least one other controller to said single endpoint communication device, said reconverted plurality of multiport packets using two or more ports associated with said multiport communication protocol.

11. A communication community comprising:

one or more shared controllers connected to one or more endpoint communication devices, wherein said one or more shared controllers is behind a firewall, and wherein said one or more shared controllers is operable to convert a plurality of multiport packets received from said one or more endpoint communication devices into a plurality of single-port packets in a single-port communication protocol;

at least one individual controller connected to a single endpoint communication device, wherein said at least one individual controller is behind another firewall, and wherein said at least one individual controller is operable to reconvert said plurality of single-port packets into said multiport communication protocol, resulting in reconverted plurality of multiport packets, and transmit to said single endpoint communication device said reconverted plurality of multiport packets using two or more ports associated with said multiport communication protocol; and

an external controller that comprises a device, said external controller in connection to said one or more shared controllers and said at least one individual controller, wherein said external controller is not behind said firewall or said another firewall, and wherein said external controller facilitates communication between ones of said one or more endpoint communication devices and said single endpoint communication device.

12. The communication community of claim 11 further comprising:

a verification utility within said external controller for verifying one or more communication requests from one or more of said one or more shared controllers and said individual controller.

13. The communication community of claim 11 further comprising:

a security key repository within each of said one or more shared controllers and said individual controller, wherein said one or more shared controllers and said individual controller transmit a security key for verification by said external controller for each communication request issued to said external controller.

14. The communication community of claim 11 further comprising:

an external communication interface within said external controller for communicating with a second communication community.

16

15. The communication community of claim 14 wherein said external controller communicates with a central communication controller to establish a communication channel with said second communication community.

16. The communication community of claim 11 wherein said one or more shared controllers, and said at least one individual controller each comprise a device.

17. A method for communicating comprising:

establishing a first communication connection between a first internal controller behind a firewall and a first external controller in a first communication community, said first external controller not behind said firewall, wherein a first communication request is initiated by a local communication device connected to the first internal controller;

establishing a second communication connection between a second internal controller behind a second firewall and a second external controller in a second communication community, said second external controller not behind said second firewall, wherein a second communication request is initiated by a remote communication device connected to the second internal controller;

responsive to one or more of the first and second communication request requesting communication between the local communication device and the remote communication device, establishing a third communication connection between the first and second external communication controllers; and

transmitting communication data between the first and second communication communities through the third communication connection, wherein said transmitting comprises:

receiving, at a first intermediate communication device that is behind said firewall a plurality of multiport packets of data in a multiport communication protocol for communication from said local communication device in said first communication community, converting, by said first intermediate communication device, said plurality of multiport packets into a plurality of single-port packets in a single-port communication protocol,

transmitting, through the third communication connection, said plurality of single-port packets to a second intermediate communication device that is behind said second firewall,

receiving said plurality of single-port packets at said second intermediate communication device,

reconverting, by said second intermediate communication device, said received plurality of single-port packets into said multiport communication protocol, resulting in reconverted plurality of multiport packets, and

delivering, from said second intermediate communication device to said remote communication device in said second communication community, said reconverted plurality of multiport packets using two or more ports associated with said multiport communication protocol.

18. The method of claim 17 further comprising:

verifying at said first external controller said first communication request prior to said establishing said first communication connection; and

verifying at said second external controller said second communication request prior to said establishing said second communication connection.

19. The method of claim 18 further comprising:

US 8,560,828 B2

17

issuing a third communication request between said first and second external controllers; and  
verifying said third communication request prior to said establishing said third communication connection.  
20. The method of claim 17 wherein said establishing a third communication connection comprises:  
issuing a third communication request to a central communication controller;  
establishing a first central communication channel between said first external controller and said central communication controller;  
issuing a fourth communication request from said central communication controller to said second external controller; and  
establishing a second central communication channel between said central communication controller and said second external controller.  
21. The method of claim 20 further comprising:

18

verifying said third communication request at said central communication controller prior to said establishing said first central communication channel;  
verifying said fourth communication request prior to said establishing said second central communication channel.  
22. The method of claim 17 wherein said first internal controller comprises said first intermediate communication device; and wherein said second internal controller comprises said second intermediate communication device.  
23. The method of claim 17 wherein said transmitting, through the third communication connection, said plurality of single-port packets to a second intermediate communication device that is behind said second firewall comprises:  
transmitting said plurality of single-port packets over a commonly-open port.

\* \* \* \* \*

# **EXHIBIT 5**

PTO/S&P (08-04)

Approved for use through 07/31/2008. OMB 0861-0031

U. S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

### Applicant Initiated Interview Request Form

Application No.: 11/403,549-Conf. #7831 First Named Applicant: Christopher S. Signaoff  
Examiner: Dargaye H. Chumet Art Unit: 2619 Status of Application: Pending

**Tentative Participants:**

- (1) Jody Bishop (2) Christopher S. Signaoff  
(3) Justin S. Signaoff (4) Tom Opsahl  
(5) Examiner: Dargaye H. Chumet (6) Supervisor: Chirag Shah

Proposed Date of Interview: April 14, 2009 Proposed Time: 2:00 (PM) (Eastern Time)

**Type of Interview Requested:**

- (1) ☒ Telephonic (2) ☐ Personal (3) ☐ Video Conference

Exhibit To Be Shown or Demonstrated: ☐ YES ☒ NO

If yes, provide brief description: \_\_\_\_\_

### Issues To Be Discussed

| Issues<br>(Rej., Obj., etc) | Claims/<br>Fig. #s  | Prior<br>Art   | Discussed                | Agreed                   | Not Agreed               |
|-----------------------------|---|--|--------------------------|--------------------------|--------------------------|
| (1) <u>35 USC 103</u>       | <u>Figs 1-3 and Fig<br/>Representing<br/>Yim's Solution</u> | <u>Yim (U.S. Pat.<br/>App. Pub. No.<br/>2006/0104288)</u>                        | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| (2) <u>35 USC 103</u>       | <u>Claim 21</u>   | <u>Yim and<br/>Adusimilli (U.S.<br/>Pat. App. Pub.<br/>No.<br/>2003/0081783)</u> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

☒ Continuation Sheet Attached

**Brief Description of Arguments to be Presented:**

See Continuation Sheet attached.

An interview was conducted on the above-identified application on \_\_\_\_\_

**NOTE:**

This form should be completed by applicant and submitted to the examiner in advance of the interview (see MPEP 5713.01).

This application will not be delayed from issue because of applicant's failure to submit a written record of this interview. Therefore, applicant is advised to file a statement of the substance of this interview (37 CFR 1.133(b)) as soon as possible.

\_\_\_\_\_  
Applicant/Applicant's Representative Signature

\_\_\_\_\_  
Examiner/SPE Signature

Jody Bishop

\_\_\_\_\_  
Typed/Printed Name of Applicant or Representative

44,034

\_\_\_\_\_  
Registration Number, if applicable

65288307.1

PTO/SB/97 (09-04)

Approved for use through 07/31/2008. OMB 0651-0031  
U. S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Applicant would like to discuss Figures 1-3 of the present application (attached herewith), along with the attached figure that represents the solution proposed by *Yim*.

Applicant would like to direct the Examiner's attention primarily to independent claim 21 for discussion. Claim 21 recites:

21. A method comprising:

receiving at a first network device a plurality of packets of data from two or more ports, said plurality of packets having at least one original communication protocol;  
encrypting the packets, thereby resulting in encrypted packets;  
encapsulating the encrypted packets in a single-port communication protocol that is acceptable by any of a plurality of different commonly-open ports, thereby resulting in encapsulated packets;

transmitting from said first network device said encapsulated packets over a selected one of the plurality of different commonly-open ports, wherein said encapsulated packets traverse one or more firewalls between said first and second network devices using said selected one of the plurality of different commonly-open ports;

receiving at a second network device said encapsulated packets from said selected one of the plurality of different commonly-open ports;

decrypting the received encapsulated packets, thereby resulting in decrypted packets;  
restoring the decrypted packets to the at least one original communication protocol, thereby resulting in restored packets; and

distributing on from said second network device each of said restored packets to said two or more ports. (Emphasis added).

The Final Office Action rejects claim 21 under 35 USC 103 over *Yim* in view of *Adusimilli*. The Final Office Action contends that *Yim* discloses all of the limitations except the recited encrypting and decrypting, which the Final Office Action contends *Adusimilli* discloses.

However, claim 21 recites encapsulating the encrypted packets in a single-port communication protocol that is acceptable by any of a plurality of different commonly-open ports. *Yim* does not disclose such encapsulation, but instead proposes converting its packets from one protocol to another. For instance, *Yim* proposes to change the packet headers to convert the packet to a selected protocol, such as HTTP or Telnet. As will be discussed in the interview, the conversion process of *Yim* is much different than the recited encapsulation of claim 21, and the two processes yield different results.

Also, claim 21 recites "distributing on from said second network device each of said restored packets to said two or more ports." Thus, as shown in the examples of FIGURES 2 and 3 of the present application, second network device 24/34 communicates the restored packets to the two or more ports of the receiving endpoint communication device 15. There does not appear to be any such distributing in *Yim*, but rather the recipient endpoint communication device 120 of *Yim* has the modified protocol stack 122 implemented thereon for receiving the packets. Thus, in *Yim* the receiving endpoint device (120) receives the communication via the single port for which the packets are specifically converted (e.g., HTTP), and no further distributing of restored packets to two or more ports is proposed in *Yim*'s solution.

65288307.1

# **EXHIBIT 6**

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with § 1.6(a)(4).

Dated: August 26, 2009

Signature: Donna Dobson

(Donna Dobson)

Docket No.: 69936/P001US/10601228  
(PATENT)

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Patent Application of:  
Christopher S. Signaoff et al.

Application No.: 11/403,549

Confirmation No.: 7831

Filed: April 13, 2006

Art Unit: 2419

For: SYSTEM AND METHOD FOR TRAVERSING  
A FIREWALL WITH MULTIMEDIA  
COMMUNICATION

Examiner: A. Hsu

**AMENDMENT IN RESPONSE TO NON-FINAL OFFICE ACTION**

MS Amendment  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Dear Sir:

**INTRODUCTORY COMMENTS**

In response to the Office Action dated August 18, 2009, please amend the above-identified U.S. patent application as follows:

**Amendments to the Claims** are reflected in the listing of claims which begins on page 2 of this paper.

**Remarks/Arguments** begin on page 9 of this paper.



**AMENDMENT TO THE CLAIMS**

1. (Currently Amended) A method for communication between two or more endpoints, said method comprising:

receiving, at a first intermediate communication device that is communicatively coupled with a first endpoint communication device, a plurality of multiport packets of data in a multiport communication protocol for communication from the first endpoint communication device;

converting, by said first intermediate communication device, said plurality of multiport packets into a plurality of single-port packets in a single-port communication protocol;

transmitting from said first intermediate communication device said plurality of single-port packets over a commonly-open port to at least a second intermediate communication device that is communicatively coupled with one or more other endpoint communication devices, said plurality of single-port packets traversing one or more firewalls using said commonly-open port;

receiving said plurality of single-port packets at said at least a second intermediate communication device;

reconverting, by said at least a second intermediate communication device, said received plurality of single-port packets into said multiport communication protocol, resulting in reconverted plurality of multiport packets; and

delivering, from said at least a second intermediate communication device to said one or more other endpoint communication devices, said reconverted plurality of multiport packets using two or more ports associated with said multiport communication protocol.

2. (Original) The method of claim 1, further comprising:  
encrypting said plurality of single-port packets in said single-port communication protocol prior to said transmitting.

3. (Original) The method of claim 2, further comprising:  
decrypting said encrypted plurality of single-port packets prior to said reconverting.

4. (Original) The method of claim 2, wherein said encrypting is according to one of:

an Advanced Encryption Standard (AES) 128-bit algorithm;  
a Triple Data Encryption Standard (TDES) algorithm; or  
a Skipjack algorithm.

5. (Original) The method of claim 1, wherein:  
said single-port communication protocol comprises:  
Secure Sockets Layer (SSL) protocol.

6. (Original) The method of claim 1, wherein:  
a portion of said plurality of multiport packets conforms to a first transmission protocol of said multiport communication protocol;  
another portion of said plurality of multiport packets conforms to a second transmission protocol of said multiport communication protocol; and  
wherein said transmitting comprises transmitting said plurality of single-port packets using said first transmission protocol in said single-port communication protocol.

7. (Original) The method of claim 6, wherein said first transmission protocol comprises Transmission Control Protocol (TCP); and  
said second transmission protocol comprises User Datagram Protocol (UDP).

8. (Original) The method of claim 6, further comprising:  
sending alternate data instead of requested data in response to a resend request.

9. (Original) The method of claim 1, further comprising:  
qualifying said plurality of multiport packets, wherein said qualifying comprises:  
registering a network device;  
using network ports by said registered network device;  
determining whether said plurality of multiport packets originated from a network port used by said registered network device; and  
allowing further transmission of said plurality of multiport packets based on said determining.

Application No. 11/403,549

Docket No.: 69936/P001US/10601228

10. (Original) The method of claim 1, wherein said commonly-open port is a well-known port.

11. (Original) The method of claim 1, wherein said commonly-open port is port 443.

12. (Currently Amended) A system comprising:  
a first network device that is communicatively coupled with at least a first endpoint communication device, said first network device comprising:  
an interface for receiving a plurality of multiport packets of data in a multiport communication protocol from two or more ports for communication from said at least a first endpoint communication device; and  
a conversion table for said first network device to convert said plurality of multiport packets into a plurality of single-port packets in a single-port communication protocol, wherein said single-port communication protocol is acceptable by any of a plurality of different commonly-open transmission control protocol (TCP) ports, and wherein said interface communicates said converted plurality of single-port packets over a selected one of the plurality of different commonly-open TCP ports; and  
a second network device that is communicatively coupled with at least a second endpoint communication device, said second network device comprising:  
a second interface for receiving said converted plurality of single-port packets from said selected one of the plurality of different commonly-open TCP ports;  
a second conversion table for reconvertng said converted plurality of single-port packets into said multiport communication protocol, resulting in a reconverted plurality of multiport packets; and  
wherein said second interface distributes each of said reconverted plurality of multiport packets to said two or more ports for communication to said at least a second endpoint communication device; and  
wherein one or more firewalls are traversed between said first and second network devices using said selected one of the plurality of different commonly-open TCP ports.

13. (Original) The system of claim 12, further comprising:  
an encryption application in said first network device for encrypting said plurality of packets in said single-port communication protocol; and  
a decryption application in said second network device for decrypting said encrypted plurality of packets prior to said reconverting.

14. (Original) The system of claim 13, wherein said encrypting is according to one of:  
an Advanced Encryption Standard (AES) 128-bit algorithm;  
a Triple Data Encryption Standard (TDES) algorithm; or  
a Skipjack algorithm.

15. (Original) The system of claim 12, wherein said single-port communication protocol is Secure Sockets Layer (SSL) protocol.

16. (Original) The system of claim 12, wherein:  
a portion of said plurality of packets from said two or more ports conform to Transmission Control Protocol (TCP);  
another portion of said plurality of packets from said two or more ports conform to User Datagram Protocol (UDP); and  
wherein said single-port communication protocol uses said TCP.

17. (Original) The system of claim 12, wherein said first and second network devices send alternate data instead of requested data in response to a resend request.

18. (Currently Amended) The system of claim 12, wherein said first network device qualifies said ~~multimedia~~ multiport packets, wherein said qualifying comprises:  
registering a third network device with said first network device;  
using network ports by said third network device;  
determining whether said plurality of multiport packets originated from a network port used by said third network device; and  
allowing further transmission of said plurality of multiport packets based on said determining.

19. (Previously Presented) The system of claim 12, wherein said selected one of the plurality of different commonly-open TCP ports is a well-known port.

20. (Previously Presented) The system of claim 12, wherein said selected one of the plurality of different commonly-open TCP ports is port 443.

21. (Currently Amended) A method comprising:

receiving, at a first intermediary network device that is communicatively coupled with a source communication device, a plurality of multiport packets of data from two or more ports for communication from said source communication device, said plurality of multiport packets having at least one original communication protocol;

encrypting the plurality of multiport packets, thereby resulting in encrypted packets;

encapsulating the encrypted packets into a plurality of single-port packets in a single-port communication protocol that is acceptable by any of a plurality of different commonly-open ports, thereby resulting in encapsulated packets;

transmitting from said first intermediary network device said encapsulated packets over a selected one of the plurality of different commonly-open ports, wherein said encapsulated packets traverse one or more firewalls between said first intermediary network device and a second intermediary network device using said selected one of the plurality of different commonly-open ports;

receiving, at said second intermediary network device that is communicatively coupled with a destination communication device, said encapsulated packets from said selected one of the plurality of different commonly-open ports;

decrypting the received encapsulated packets, thereby resulting in decrypted packets;

restoring the decrypted packets to the at least one original communication protocol, thereby resulting in restored multiport packets; and

distributing, [[on]] from said second intermediary network device, each of said restored multiport packets to said two or more ports for communication to said destination communication device.

22. (Canceled)

23. (Previously Presented) The method of claim 21, wherein said encrypting is according to one of:

an Advanced Encryption Standard (AES) 128-bit algorithm;

a Triple Data Encryption Standard (TDES) algorithm; or  
a Skipjack algorithm.

24. (Original) The method of claim 21, wherein said single-port communication protocol is Secure Sockets Layer (SSL) protocol.

25. (Currently Amended) The method of claim 21, wherein:  
a portion of said plurality of multiport packets from said two or more ports conform to Transmission Control Protocol (TCP);  
another portion of said plurality of multiport packets from said two or more ports conform to User Datagram Protocol (UDP); and  
wherein said single-port communication protocol uses said TCP.

26. (Previously Presented) The method of claim 21, wherein said first and second intermediary network devices send alternate data instead of requested data in response to a resend request.

27. (Currently Amended) The method of claim 21, further comprising qualifying said ~~multimedia~~ multiport packets, wherein said qualifying comprises:  
registering a third network device with said first intermediary network device;  
determining whether said plurality of multiport packets originated from said third network device; and  
allowing further transmission of said plurality of multiport packets based on said determining.

28. (Previously Presented) The method of claim 21, wherein said selected one of the plurality of different commonly-open ports is a well-known port.

29. (Previously Presented) The method of claim 21, wherein said selected one of the plurality of different commonly-open ports is port 443.

30. (Previously Presented) The method of claim 1 wherein said single-port communication protocol is acceptable by any of a plurality of different commonly-open transmission control protocol (TCP) ports.

Application No. 11/403,549

Docket No.: 69936/P001US/10601228

31. (Previously Presented) The method of claim 1 wherein said single-port communication protocol is not hypertext transport protocol (HTTP).

## **REMARKS**

### **I. Overview**

Claims 1-21 and 23-31 were pending in this application. The current Office Action of August 18, 2009 objects to all of the claims for certain informalities, but otherwise indicates that the claims are in condition for allowance, *see* page 2 of the Office Action.

In response, Applicant respectfully submits this amendment to address the informalities, and thus respectfully submits that the application is now in condition for allowance.

### **II. Claim Amendments**

Claims 1, 12, 18, 21, 25, and 27 are amended herein.

Claim 1 is amended to recite “reconverting, by said at least a second intermediate communication device, said received plurality of single-port packets” (newly-added language shown underlined), as suggested by the Office Action. This amendment is not intended to narrow the scope of the claim in any way but is instead intended as a mere cosmetic change to refer to the plurality of single-port packets as “received.”

Claim 1 is further amended to recite “reconverting ... said ... plurality of single-port packets into said multipoint communication protocol, resulting in reconverted plurality of multipoint packets” (newly-added language shown underlined). This further amendment is likewise not intended to narrow the scope of the claim in any way but is instead intended as a mere cosmetic change. The added language establishes the “reconverted plurality of multipoint packets” as a name for use in clearly referring to these packets later in the claim.

As discussed below, in a telephone conference conducted August 27, 2009 with the Examiner, Alpus H. Hsu, Applicant’s representative, Jody Bishop, discussed revising the amendment to claim 1 proposed by the Office Action to that presented herein so as to avoid an apparent requirement that the reconverted plurality of multipoint packets necessarily be identical to the plurality of multipoint packets that are recited as being received by a first intermediate communication device. Rather, the claim recites that the single-port packets are reconverted into the multipoint communication protocol, but it does not necessarily require



that the resulting reconverted plurality of multiport packets be identical to the plurality of multiport packets that are recited as being received by a first intermediate communication device. Thus, the resulting reconverted plurality of multiport packets may be identical to or may differ in some way (*e.g.*, have additional information included therein, etc.) from the plurality of multiport packets that are recited as being received by a first intermediate communication device.

Claim 1 is further amended, as suggested by the Office Action, to recite “delivering, from said at least a second intermediate communication device to said one or more other endpoint communication devices, said reconverted plurality of multiport packets using two or more ports ...” (newly-added language shown underlined). This further amendment is likewise not intended to narrow the scope of the claim in any way but is instead intended as a mere cosmetic change. The added language merely utilizes “reconverted” in the name for clearly referring to the packets resulting from the reconverting operation earlier recited in the claim.

Claim 12 is amended, as suggested by the Office Action, to recite “an interface for receiving a plurality of multiport packets of data in a multiport communication protocol from two or more ports ...” (newly-added language shown underlined). This amendment is not intended to narrow the scope of claim 12 in any way but is instead intended as a mere cosmetic change. As confirmed by Applicant’s representative with the Examiner during the conference of August 27, 2009 (summarized below), the added language is not intended to narrow the claim in any way. Instead, the recitation of the packets as being “multiport” packets that are “in a multiport communication protocol” merely reiterates that the packets of data are received from two or more ports, as the claim previously recited. Thus, while the added language adds a naming convention for use in the claim, by referring to the packets as being “multiport” packets, this naming convention does not narrow the scope of the claim in any way.

Claim 12 is further amended, as suggested by the Office Action, to recite “a conversion table for said first network device to convert said plurality of multiport packets into a plurality of single-port packets in a single-pot communication protocol ...” (newly-added language shown underlined). This amendment is likewise not intended to narrow the scope of claim 12 in any way but is instead intended as a mere cosmetic change. As

discussed above, the use of “multiport” packets is merely a non-narrowing naming convention. Further, as confirmed by Applicant’s representative with the Examiner during the conference of August 27, 2009 (summarized below), the added language is not intended to narrow the claim in any way. Instead, the recitation of the packets as being “single-port” packets merely reiterates that the packets of data are communicated over a selected one of the plurality of different commonly-open TCP ports, as the claim later recites. Thus, while the added language adds a naming convention for use in the claim, by referring to the packets as being “single-port” packets, this naming convention does not narrow the scope of the claim in any way. Further amendments are also made in claim 12, as suggested by the Office Action, to consistently use the non-narrowing “single-port” packets naming convention.

Claim 12 is further amended to recite “a second conversion table for reconvertng said converted plurality of single-port packets into said multiport communication protocol, resulting in a reconverted plurality of multiport packets” (newly-added language shown underlined). This further amendment is likewise not intended to narrow the scope of the claim in any way but is instead intended as a mere cosmetic change. The added language establishes the “reconverted plurality of multiport packets” as a name for use in clearly referring to these packets later in the claim.

As mentioned above with claim 1, in a telephone conference conducted August 27, 2009 with the Examiner, Alpus H. Hsu, Applicant’s representative, Jody Bishop, discussed revising the amendment proposed by the Office Action to that presented herein so as to avoid an apparent requirement that the reconverted plurality of multiport packets necessarily be identical to the plurality of multiport packets that are recited as being received by the interface of the first network device. Thus, as recited in claim 12, the resulting reconverted plurality of multiport packets may be identical to or may differ in some way (*e.g.*, have additional information included therein, etc.) from the plurality of multiport packets that are recited as being received by the interface of the first network device.

In addition, dependent claim 18 is amended herein for consistency with the above-mentioned “multiport” packets naming convention of claim 12 from which claim 18 depends, and to change “said multimedia packets” to “said multiport packets” to ensure that proper antecedent basis exists for this phrase.

Claim 21 is amended as suggested by the Office Action to recite “a plurality of multiport packets of data from two or more ports ...” (newly-added language shown underlined). This amendment is not intended to narrow the scope of claim 21 in any way but is instead intended as a mere cosmetic change. As confirmed by Applicant’s representative with the Examiner during the conference of August 27, 2009 (summarized below), the added language is not intended to narrow the claim in any way. Instead, the recitation of the packets as being “multiport” packets merely reiterates that the packets of data are received from two or more ports, as the claim recites. Thus, while the added language adds a naming convention for use in the claim, by referring to the packets as being “multiport” packets, this naming convention does not narrow the scope of the claim in any way.

Claim 21 is further amended to recite “encrypting the plurality of multiport packets” (newly-added language shown underlined) for consistency with the above-mentioned naming convention. This does not narrow the scope of claim 21 in any way, but instead merely uses the non-narrowing naming convention of “plurality of multiport” packets. It is noted that the claim previously recited “encrypting the packets”, which clearly referred to the plurality of packets of data from two or more ports (*i.e.*, the now-named “multiport” packets). Thus, this amendment does not narrow the scope of the claim in any way whatsoever. Further amendments are presented in claim 21 to consistently use the “multiport” packets naming convention, and those amendments likewise do not narrow the scope of the claim but are instead mere cosmetic changes.

Claim 21 is further amended to recite “encapsulating the encrypted packets into a plurality of single-port packets in a single-port communication protocol” (newly-added language shown underlined). As confirmed by Applicant’s representative with the Examiner during the conference of August 27, 2009 (summarized below), the added language is not intended to narrow the claim in any way. Instead, the recitation of the packets as being a plurality of “single-port” packets merely reiterates that the packets are transmitted over a selected one of the plurality of different commonly-open ports, as the claim later recites. Thus, while the added language adds a naming convention for use in the claim, by referring to the packets as being “single-port” packets, this naming convention does not narrow the scope of the claim in any way.

Claim 21 is also amended to insert “intermediary” between “a second” and “network device” to properly establish antecedent basis for the later-recited “said second intermediary network device”. This is not intended to narrow the recited limitation in any way, but instead merely corrects a clear typographical error in the claim to properly refer to a second intermediary network device.

Claim 21 is also amended to delete an unnecessary “on” and to insert two commas. These amendments are likewise not intended to narrow the scope of the claim in any way whatsoever, but are instead merely intended as cosmetic changes that improve the readability of the claim.

In addition, dependent claim 25 is amended herein for consistency with the above-mentioned “multiport” packets naming convention of claim 21 from which claim 25 depends. This amendment is not intended to narrow the scope of claim 25.

And, dependent claim 27 is amended herein for consistency with the above-mentioned “multiport” packets naming convention of claim 21 from which claim 27 depends, and to change “said multimedia packets” to “said multiport packets” to ensure that proper antecedent basis exists for this phrase. Again, this amendment is not intended as a narrowing amendment to claim 27.

Applicant respectfully notes that none of the amendments presented herein are intended to be narrowing of the claims, and they amendments are not made to overcome any prior art, as the claims are indicated as being allowable over the prior art by the current Office Action. Rather, the amendments are made solely to make cosmetic changes to address the asserted informalities noted by the Office Action.

### **III. Record of Conference with the Examiner**

A telephone conference was conducted on August 27, 2009 between the Examiner, Alpus H. Hsu, and Applicant’s representative, Jody Bishop. Applicant thanks the Examiner for his time and consideration in discussing the remaining minor informalities asserted by the current Office Action.

Application No. 11/403,549

Docket No.: 69936/P001US/10601228

The Examiner confirmed that the above-mentioned naming conventions of “multiport” packets and “single-port” packets added in the amendments presented herein, are not intended as narrowing amendments but are instead merely naming conventions for referring to the packets without imposing any additional requirements or limitations on the packets as otherwise recited.

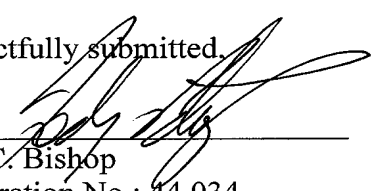
In addition, the Examiner and Applicant’s representative discussed revising the amendment to claim 1 from that proposed by the Office Action to that presented herein so as to avoid an apparent requirement that the reconverted plurality of multiport packets necessarily be identical to the plurality of multiport packets that are recited as being received by a first intermediate communication device. Thus, the resulting reconverted plurality of multiport packets as recited by amended claim 1 may be identical to or may differ in some way (*e.g.*, have additional information included therein, etc.) from the plurality of multiport packets that are recited as being received by a first intermediate communication device.

#### **IV. Conclusion**

In view of the above, Applicant believes the pending application is in condition for allowance. Applicant believes no fee is due with this response. Please charge any fees required or credit any overpayment to Deposit Account No. 06-2380, under Order No. 69936/P001US/10601228 during the pendency of this Application pursuant to 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees.

Dated: August 28, 2009

Respectfully submitted,

By   
Jody C. Bishop  
Registration No.: 44,034  
FULBRIGHT & JAWORSKI L.L.P.  
2200 Ross Avenue, Suite 2800  
Dallas, Texas 75201-2784  
(214) 855-8007  
(214) 855-8200 (Fax)  
Attorney for Applicant

# **EXHIBIT 7**

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with § 1.6(a)(4).

Dated: August 19, 2008

Signature:

  
(Donna Forbit)

Docket No.: 69936/P003US/10601230  
(PATENT)

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Patent Application of:  
Christopher S. Signaoff et al.

Application No.: 11/403,552

Confirmation No.: 7846

Filed: April 13, 2006

Art Unit: 2616

For: SYSTEM AND METHOD FOR CROSS  
PROTOCOL COMMUNICATION

Examiner: T. R. Phan

**AMENDMENT IN RESPONSE TO NON-FINAL OFFICE ACTION**

MS Amendment  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Dear Sir:

**INTRODUCTORY COMMENTS**

In response to the Office Action dated May 21, 2008, please amend the above-identified U.S. patent application as follows:

**Amendments to the Claims** are reflected in the listing of claims which begins on page 2 of this paper.

**Remarks/Arguments** begin on page 9 of this paper.

AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method for multimedia communication comprising:
  - receiving a multimedia data stream at a communication controller in a first protocol from a communication device, wherein the first protocol comprises a signaling protocol;
  - detecting a type of said first protocol;
  - converting said first protocol into an intermediate protocol;
  - translating said intermediate protocol into a second protocol, wherein the second protocol comprises a signaling protocol; and
  - transmitting said multimedia data stream in said second protocol to a target communication device.
2. (Currently Amended) The method of claim 1 further comprising:
  - communicating, prior to said translating, said multimedia data stream in said ~~intermediate~~ communication controller to a second communication controller connected to said target communication device; wherein said translating and said transmitting are performed by said second communication controller.
3. (Original) The method of claim 1 wherein said converting comprises:
  - accessing a first protocol table responsive to said type, wherein said first protocol table includes a plurality of first protocol messages corresponding to a plurality of intermediate protocol messages;
  - selecting ones of said plurality of intermediate protocol messages that correspond to one or more first protocol messages found in said multimedia data stream; and
  - assembling said ones of said plurality of intermediate protocol messages to form said multimedia data stream in said intermediate protocol.



Application No. 11/403,552

Docket No.: 69936/P003US/10601230

4. (Original) The method of claim 1 wherein said translating comprises:  
determining a second protocol type associated with said target communication device;  
accessing a second protocol table responsive to said second protocol type, wherein said second protocol table includes a plurality of second protocol messages corresponding to said plurality of intermediate protocol messages;  
selecting ones of said plurality of second protocol messages that correspond to one or more intermediate protocol messages found in said multimedia data stream; and  
assembling said ones of said plurality of second protocol messages to form said multimedia data stream in said second protocol.

5. (Original) The method of claim 4 further comprising:  
retrieving said second protocol type from a device information base, wherein said device information base contains compatibility information for each device available for said multimedia communication.

6. (Original) The method of claim 1 wherein said first protocol comprises one of a text-based protocol and a binary protocol and wherein said second protocol comprises one of a binary protocol and a text-based protocol.

7. (Original) The method of claim 6 wherein said intermediate protocol comprises protocol messages common to said text-based protocol and said binary protocol.

8. (Currently Amended) A communication controller in a multimedia communication system, said communication controller comprising:

- a message interface to transceive multimedia data from a communication endpoint in a first protocol, wherein the first protocol comprises a signaling protocol;
- a protocol signaler to determine a type of said first protocol;
- a first protocol conversion table that contains a plurality of first protocol messages and a plurality of interim protocol messages, wherein said plurality of interim protocol messages correspond to ones of said plurality of first protocol messages;
- a protocol conversion utility to convert said first protocol into an interim protocol using said first protocol conversion table; and
- a network interface to transceive said multimedia data in said interim protocol to a target communication endpoint.

9. (Original) The communication controller of claim 8 wherein said protocol conversion utility converts said interim protocol of a received multimedia data stream into a second protocol and wherein said message interface transmits said received multimedia data stream in said second protocol to a destination endpoint connected to said communication controller.

10. (Original) The communication controller of claim 9 further comprising:

- a second protocol conversion table that contains a plurality of second protocol messages and said plurality of interim protocol messages, wherein said plurality of interim protocol messages correspond to ones of said plurality of second protocol messages.

11. (Original) The communication controller of claim 9 further comprising:

- an endpoint information base including compatibility data on one or more communication endpoints connected to said communication controller, wherein said compatibility data includes a device protocol type.

Application No. 11/403,552

Docket No.: 69936/P003US/10601230

12. (Currently Amended) A method for multimedia communication comprising:

receiving a multimedia data stream at a communication controller in a first protocol from a communication device;

detecting a type of said first protocol;

converting said first protocol into an intermediate protocol, wherein said converting is performed irrespective of a second protocol in which the multimedia data stream is to be transmitted to a target communication device;

translating said intermediate protocol into ~~[[a]]~~ said second protocol; and

transmitting said multimedia data stream in said second protocol to ~~[[a]]~~ the target communication device.

13. (Currently Amended) The method of claim 12 further comprising:  
communicating, prior to said translating, said multimedia data stream in said ~~intermediate~~ communication controller to a second communication controller connected to said target communication device; wherein said translating and said transmitting are performed by said second communication controller.

14. (Original) The method of claim 12 wherein said converting comprises:  
accessing a first protocol table responsive to said type, wherein said first protocol table includes a plurality of first protocol messages corresponding to a plurality of intermediate protocol messages;  
selecting ones of said plurality of intermediate protocol messages that correspond to one or more first protocol messages found in said multimedia data stream; and  
assembling said ones of said plurality of intermediate protocol messages to form said multimedia data stream in said intermediate protocol.

15. (Original) The method of claim 12 wherein said translating comprises:  
determining a second protocol type associated with said target communication device;  
accessing a second protocol table responsive to said second protocol type, wherein said second protocol table includes a plurality of second protocol messages corresponding to said plurality of intermediate protocol messages;  
selecting ones of said plurality of second protocol messages that correspond to one

or more intermediate protocol messages found in said multimedia data stream; and  
assembling said ones of said plurality of second protocol messages to form said multimedia data stream in said second protocol.

16. (Original) The method of claim 15 further comprising:  
retrieving said second protocol type from a device information base, wherein said device information base contains compatibility information for each device available for said multimedia communication.

17. (Original) The method of claim 12 wherein said first protocol comprises one of a text-based protocol and a binary protocol and wherein said second protocol comprises one of a binary protocol and a text-based protocol.

18. (Original) The method of claim 17 wherein said intermediate protocol comprises protocol messages common to said text-based protocol and said binary protocol.

19. (Currently Amended) A computer program product having a computer readable storage medium with computer program logic recorded thereon for multimedia communication, said computer program product comprising:  
code for receiving a multimedia data stream at a communication controller in a first protocol from a communication device;  
code for detecting a type of said first protocol;  
code for converting said first protocol into an intermediate protocol, wherein said converting is performed irrespective of a second protocol in which the multimedia data stream is to be transmitted to a target communication device;  
code for translating said intermediate protocol into [[a]] the second protocol; and  
code for transmitting said multimedia data stream in said second protocol to [[a]] the target communication device.

20. (Currently Amended) The computer program product of claim 19 further comprising:  
code for communicating, prior to execution of said code for translating, said multimedia data stream in said ~~intermediate~~ communication controller to a second communication controller connected to said target communication device; wherein said

Application No. 11/403,552

Docket No.: 69936/P003US/10601230

code for translating and said code for transmitting are executed at said second communication controller.

21. (Original) The computer program product of claim 19 wherein said code for converting comprises:

code for accessing a first protocol table responsive to said type, wherein said first protocol table includes a plurality of first protocol messages corresponding to a plurality of intermediate protocol messages;

code for selecting ones of said plurality of intermediate protocol messages that correspond to one or more first protocol messages found in said multimedia data stream; and

code for assembling said ones of said plurality of intermediate protocol messages to form said multimedia data stream in said intermediate protocol.

22. (Original) The computer program product of claim 19 wherein said code for translating comprises:

code for determining a second protocol type associated with said target communication device;

code for accessing a second protocol table responsive to said second protocol type, wherein said second protocol table includes a plurality of second protocol messages corresponding to said plurality of intermediate protocol messages;

code for selecting ones of said plurality of second protocol messages that correspond to one or more intermediate protocol messages found in said multimedia data stream; and

code for assembling said ones of said plurality of second protocol messages to form said multimedia data stream in said second protocol.

23. (Original) The computer program product of claim 22 further comprising:

code for retrieving said second protocol type from a device information base, wherein said device information base contains compatibility information for each device available for said multimedia communication.

Application No. 11/403,552

Docket No.: 69936/P003US/10601230

24. (Original) The computer program product of claim 19 wherein said first protocol comprises one of a text-based protocol and a binary protocol and wherein said second protocol comprises one of a binary protocol and a text-based protocol.

25. (Original) The computer program product of claim 24 wherein said intermediate protocol comprises protocol messages common to said text-based protocol and said binary protocol.

26. (Newly Added) The method of claim 12 wherein said first protocol comprises a signaling protocol, and wherein said second protocol comprises a signaling protocol.

## REMARKS

### **I. Overview**

Claims 1-25 were pending in this application. The issues raised in the Office Action of May 21, 2008 (*Office Action*) are as follows:

- Claims 12-18 are objected to as being a substantial duplicate of claims 1-7.
- Claims 19-25 are rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter;
- Claims 2, 5, 11, 13, 16, 20, and 23 are rejected under 35 U.S.C. § 112, second paragraph as being indefinite;
- Claims 1-7 and 12-25 are rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 7,346,076 to Habiby et al.(hereinafter “*Habiby*”).
- Claims 8-11 are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,963,583 to Foti (hereinafter “*Foti*”) in view of *Habiby*.

In response, Applicant respectfully traverses all claim rejections and requests reconsideration and withdrawal in light of the amendments and remarks presented herein.

### **II. Claim Amendments**

Claims 1, 2, 8, 12, 13, 19, and 20 are amended herein, and new claim 26 is added.

Independent claim 1 is amended to recite “wherein the first protocol comprises a signaling protocol” and “wherein the second protocol comprises a signaling protocol”. No new matter is added by these amendments because the specification clearly discloses use of such signaling protocols as H.323 and Session Initiation Protocol (SIP), *see e.g.*, paragraphs 0002-0005 and 0017-0025 of the specification.

Claim 2 is amended to change “intermediate controller” to “communication controller” for consistency with terminology introduced in independent claim 1, from which claim 2 depends.

Independent claim 8 is amended to recite “wherein the first protocol comprises a signaling protocol”. As discussed above with claim 1, no new matter is added by this amendment because the specification clearly supports use of various signaling protocols.

Independent claim 12 is amended to recite “wherein said converting is performed irrespective of a second protocol in which the multimedia data stream is to be transmitted to a target communication device”. No new matter is added by this amendment because the specification clearly discloses such conversion of a data stream to be transmitted irrespective of a protocol of a target communication device, *see e.g.*, description of FIGURES 2-3 in paragraphs 0021-0026 (where the conversion from a first protocol to an intermediate protocol is described as being performed irrespective of the second protocol used for communication to a target communication device).

Claim 13 is amended to change “intermediate controller” to “communication controller” for consistency with terminology introduced in independent claim 12, from which claim 13 depends.

Independent claim 19 is amended herein to recite: “A computer program product having a computer readable storage medium with computer program logic recorded thereon ...” (newly added language shown underlined). Thus, this makes clear that the computer program product has a computer readable “storage” medium with computer program logic recorded thereon. As such, this ensures that claim 19 is not directed to a transitory, propagating signal, but rather recites a statutory computer readable “storage” medium to which the computer program logic is recorded. No new matter is added by this amendment, as support for such a tangible computer readable storage medium can be found in the specification as originally filed, *see e.g.*, paragraphs 0030-0032 of the specification.

Independent claim 19 is further amended to recite “wherein said converting is performed irrespective of a second protocol in which the multimedia data stream is to be transmitted to a target communication device”. As discussed above with claim 12, no new matter is added by this amendment.



Claim 20 is amended to change “intermediate controller” to “communication controller” for consistency with terminology introduced in independent claim 19, from which claim 20 depends.

New claim 26 is introduced, which recites “wherein said first protocol comprises a signaling protocol, and wherein said second protocol comprises a signaling protocol.” No new matter is added by this new claim because it these elements are supported by the specification, as discussed above with claim 1.

### **III. Objection to Duplicate Claims**

The objection raised for claims 12-18 as being a substantial duplicate of claims 1-7 is believed to be moot in view of the amendments presented herein. Thus, this objection should be withdrawn.

### **IV. Rejections Under 35 U.S.C. §101**

Claims 19-25 are rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter because the Office Action appears to assert that the specification (paragraph 0030) of the present application defines computer readable medium in a way that encompasses non-statutory subject matter, such as a “signal per se”. That is, the Examiner appears to contend that the term “computer readable medium” is described in paragraph 0030 of the specification to be so broad as to encompass non-statutory subject matter under 35 U.S.C. §101. For instance, computer readable medium is described in paragraph 0030 as encompassing both tangible storage mediums, such as “an electronic circuit, a semiconductor memory device, a ROM, a flash memory, an erasable ROM (EROM), a floppy diskette, a compact disk CD-ROM, an optical disk, a hard disk”, as well as intangible transmission mediums such as a radio frequency (RF) link, air, etc.

In response, Applicant has amended claim 19 in the manner discussed above, which focuses the claim to a “computer readable storage medium,” which Applicant respectfully submits brings the claim under the clear statutory realm of tangible computer readable storage mediums, such as those identified in paragraphs 0030-0032 of the specification, rather than encompassing the intangible transmission mediums that are mentioned in

paragraph 0030. Applicant respectfully asserts this amendment overcomes the Examiner's rejection and renders claims 19-25 directed to statutory subject matter under 101.

Therefore, the rejection of claims 19-25 under 35 U.S.C. §101 should be withdrawn.

**V. Rejections Under 35 U.S.C. §112, Second Paragraph**

Claims 2, 5, 11, 13, 16, 20, and 23 are rejected under 35 U.S.C. §112, second paragraph, as being indefinite. Claims 2, 13, and 20 are rejected for their recitation of "said intermediate controller" without sufficient antecedent basis for that term. Those claims are amended herein to instead refer to "said communication controller", for which proper antecedent basis does exist. Therefore, the rejection of claims 2, 13, and 20 should be withdrawn.

Claims 5, 17, and 23 are rejected for their recitation of "device". The Examiner asserts that the term "device" is vague and unclear because the examiner is unclear whether this refers to the recited "communication device" or "target device". Applicant respectfully submits that the term "device" is sufficiently clear in the claim. The term does not attempt to refer to one of the prior-recited devices, such as "communication device" or "target device", but is instead sufficiently broad to encompass any or all such devices. For instance, the claims do not recite "the device" (which raises a question as to which of "the" previously-recited devices the term might be referencing), but instead the mere use of "device" in the claims is sufficiently broad to encompass any device available for multimedia communication. The Examiner is respectfully reminded that breadth is not indefiniteness, and thus merely because the term "device" is sufficiently broad to encompass one or both of the recited "communication device" and "target device" does not render use of this term indefinite. Therefore, the rejection of claims 5, 17, and 23 should be withdrawn.

Claim 11 is rejected for its recitation of "communication endpoints". The Examiner asserts that the term is vague and unclear because the examiner is unclear whether this refers to the recited "communication endpoint" or "target communication endpoint". Applicant respectfully submits that the term "communication endpoints" is sufficiently clear in the claim. The term does not attempt to refer to one of the prior-recited endpoints, such as "the communication endpoint" or "the target communication endpoint", but is instead sufficiently broad to encompass any or all such communication endpoints. That is, both the recited

“communication endpoint” and the “target communication endpoint” qualify as “communication endpoints”. The mere use of “communication endpoints” in claim 11 is sufficiently broad to encompass any such communication endpoint. The Examiner is respectfully reminded that breadth is not indefiniteness, and thus merely because the term “communication endpoints” is sufficiently broad to encompass one or both of the recited “communication endpoint” and “target communication endpoint” does not render use of this term indefinite. Therefore, the rejection of claim 11 should be withdrawn.

## **VI. Rejections Under 35 U.S.C. §102 over *Habiby***

Claims 1-7 and 12-25 are rejected under 35 U.S.C. §102(e) as being anticipated by *Habiby*. Applicant respectfully traverses these rejections for the reasons below.

To anticipate a claim under 35 U.S.C. § 102, a single reference must teach each and every element of the claim. *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631 (Fed. Cir. 1987). In fact, “[t]he identical invention must be shown in as complete detail as is contained in the . . . claim.” *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236 (Fed. Cir. 1989). Furthermore, for a reference to be anticipatory, “[its] elements must be arranged as required by the claim.” *In re Bond*, 910 F.2d 831 (Fed. Cir. 1990), *cited in* M.P.E.P. § 2131. As discussed below, *Habiby* fails to teach all elements of claims 1-7 and 12-25, and therefore fails to anticipate the claims under 35 U.S.C. §102.

### Independent Claim 1

As amended herein, claim 1 recites, in part, “receiving a multimedia data stream at a communication controller in a first protocol from a communication device, wherein the first protocol comprises a signaling protocol; detecting a type of said first protocol; converting said first protocol into an intermediate protocol;...” (emphasis added). As discussed further below, *Habiby* fails to disclose converting a first protocol that comprises a signaling protocol into an intermediate protocol.

*Habiby* appears to generally describe use of gateways to perform bearer format conversion, enabling a call to pass between networks using different internal bearer formats, *see* col. 3, lines 34-39. In discussing its Figure 1, *Habiby* explains that the format of the bearer traffic between originating node 12 and ingress gateway 22 is “bearer format 1”; the

format of the bearer traffic between ingress and egress gateways 22, 24 is “bearer format 2”; and the format of the bearer traffic between egress gateway 24 and terminating node 14 is “bearer format 3”, *see* col. 3, line 64 - col. 4, line 3.

However, at col. 7, lines 27-43, *Habiby* distinguishes the “bearer traffic” from “signaling protocols”, such as H.323 and SIP. For instance, *Habiby* states that “In order for controllers 26, 28 to exchange the necessary format conversion information, standard messages found in the Bearer Independent Call Control (BICC) signaling protocol may be used”; and “Other signaling protocols, including Session Initiation Protocol (SIP), SIP-T, H.323, PNNI, and B-ISUP, may also be used.” Col. 7, lines 27-32. Thus, while *Habiby* mentions conversion of its bearer traffic, it does not propose any conversion of the “signaling protocol” messages. Instead, *Habiby* proposes use of such signaling protocol messages to determine the appropriate conversion of the “bearer traffic”. That is, the signaling protocol messages themselves are not converted in *Habiby*, but are instead used to exchange conversion information for converting the bearer traffic.

Thus, *Habiby* fails to teach converting a first protocol to an intermediate protocol, where the first protocol comprises a signaling protocol, as recited by claim 1.

In addition, *Foti* appears to discuss conversion of various different signaling protocols, such as SIP and H.323, *see e.g.*, col. 1, line 5 - col. 3, line 67. However, the Examiner concedes in the Office Action that *Foti* does not disclose conversion of a first protocol into an interim protocol, *see* page 9 of the Office Action. The Office Action contends that *Habiby* discloses such a conversion to an interim protocol, but as discussed above, *Habiby* does not propose any such conversion of its signaling protocols (but instead only uses the signaling protocol information for converting its bearer traffic). Thus, *Habiby* does not teach or suggest conversion of a signaling protocol at all, and *Foti* does not teach or suggest conversion of a signaling protocol to an interim protocol. Accordingly, it appears that claim 1, as amended herein, is also not unpatentable under 35 U.S.C. §103(a) over the combination of *Habiby* and *Foti* for at least this reason.

In view of the above, the rejection of claim 1 should be withdrawn.

Independent Claim 12

As amended herein, claim 12 recites, in part, “converting said first protocol into an intermediate protocol, wherein said converting is performed irrespective of a second protocol in which the multimedia data stream is to be transmitted to a target communication device; translating said intermediate protocol into said second protocol; and transmitting said multimedia data stream in said second protocol to the target communication device” (emphasis added). As discussed further below, *Habiby* fails to disclose performing its converting irrespective of a second protocol in which the multimedia data stream is to be transmitted to a target communication device.

*Habiby* appears to describe a system in which a determination is made as to whether to perform its conversion based on first determining the bearer format of a target communication device. For instance, at col. 2, line 62 – col. 3, line 5, *Habiby* explains:

To efficiently determine which, if any, bearer format conversion must occur for a particular communication channel over paths 18, 20, the gateway controllers 26, 28 determine the bearer format used at each of the nodes. If, for example, an originating node 12 uses an IP protocol and terminating node 14 uses a TDM protocol, then a conversion is performed between IP and TDM somewhere along the communication path. If the originating and terminating nodes use the same bearer format as that used by the backbone network 16, then no conversion is required or performed.

Thus, *Habiby* does not teach performing its “irrespective of a second protocol in which the multimedia data stream is to be transmitted to a target communication device”, but instead expressly teaches that it determines whether to perform its conversion based on knowledge of the bearer formats of the originating and terminating nodes.

Therefore, *Habiby* fails to anticipate claim 12, and thus the rejection of claim 12 should be withdrawn.

Independent Claim 19

As amended herein, claim 19 recites, in part, “code for converting said first protocol into an intermediate protocol, wherein said converting is performed irrespective of a second protocol in which the multimedia data stream is to be transmitted to a target communication device; code for translating said intermediate protocol into the second protocol; and code for transmitting said multimedia data stream in said second protocol to the target communication device” (emphasis added). As discussed above with claim 12, *Habiby* fails to disclose performing its converting irrespective of a second protocol in which the multimedia data stream is to be transmitted to a target communication device. Therefore, *Habiby* fails to anticipate claim 19, and thus the rejection of claim 19 should be withdrawn.

Dependent Claims 2-7, 13-18, and 20-25

Each of dependent claims 2-7, 13-18, and 20-25 depends either directly or indirectly from one of independent claims 1, 12, and 19, and thus each inherits all limitations of the respective independent claim from which it depends. It is respectfully submitted that dependent claims 2-7, 13-18, and 20-25 are allowable not only because of their dependency from their respective independent claim for the reasons discussed above, but also in view of their novel claim features (which both narrow the scope of the particular claims and compels a broader interpretation of their respective independent claim).

**VII. Rejections Under 35 U.S.C. §103 over *Foti* in view of *Habiby***

Claims 8-11 are rejected under 35 U.S.C. §103(a) as being obvious over *Foti* in view of *Habiby*. Applicant respectfully traverses this rejection as provided further below.

The test for non-obvious subject matter is whether the differences between the subject matter and the prior art are such that the claimed subject matter as a whole would have been obvious to a person having ordinary skill in the art to which the subject matter pertains. The United States Supreme Court in Graham v. John Deere and Co., 383 U.S. 1 (1966) set forth the factual inquiries which must be considered in applying the statutory test: (1) determining of the scope and content of the prior art; (2) ascertaining the differences between the prior art and the claims at issue; and (3) resolving the level of ordinary skill in the pertinent art. As

discussed further hereafter, Applicant respectfully asserts that the claims include non-obvious differences over the cited art.

As discussed further below, the rejections should be overturned because when considering the scope and content of the applied *Foti* and *Habiby* references there are significant differences between the applied combination and claims 8-11, as the applied combination fails to disclose all elements of these claims. Thus, considering the lack of disclosure in the applied combination of all elements of claims 8-11, one of ordinary skill in the art would not find these claims obvious under 35 U.S.C. §103, and therefore the rejections should be withdrawn.

#### Independent Claim 8

Claim 8, as amended herein, recites:

A communication controller in a multimedia communication system, said communication controller comprising:

a message interface to transceive multimedia data from a communication endpoint in a first protocol, wherein the first protocol comprises a signaling protocol;

a protocol signaler to determine a type of said first protocol;

a first protocol conversion table that contains a plurality of first protocol messages and a plurality of interim protocol messages, wherein said plurality of interim protocol messages correspond to ones of said plurality of first protocol messages;

a protocol conversion utility to convert said first protocol into an interim protocol using said first protocol conversion table; and

a network interface to transceive said multimedia data in said interim protocol to a target communication endpoint. (Emphasis added).

Thus, claim 8 recites that a first protocol comprises a signaling protocol, and further recites a protocol conversion utility to convert said first protocol into an interim protocol. The applied combination of *Foti* and *Habiby* fails to teach or suggest these elements of claim 8, as discussed below.

As discussed above, *Habiby* does not teach or suggest converting a protocol that comprises a signaling protocol into an interim protocol. Instead, *Habiby* uses signaling protocol information for converting bearer traffic, but does not disclose any conversion of its signaling protocol.

*Foti*, on the other hand, appears to discuss conversion of various different signaling protocols, such as SIP and H.323, *see e.g.*, col. 1, line 5 - col. 3, line 67. However, the Examiner concedes in the Office Action that *Foti* does not disclose conversion of a first protocol into an interim protocol, *see* page 9 of the Office Action. The Office Action relies on *Habiby* as disclosing such a conversion to an interim protocol.

However, as discussed above, *Habiby* does not propose any such conversion of its signaling protocol (but instead only uses the signaling protocol information for converting its bearer traffic). Thus, *Habiby* does not teach or suggest conversion of a signaling protocol at all, and *Foti* does not teach or suggest conversion of a signaling protocol to an interim protocol.

Accordingly, the applied combination of *Foti* and *Habiby* does not teach or suggest the above elements of claim 8, as neither reference teaches or suggests conversion of a protocol that comprises a signaling protocol into an interim protocol. Therefore, the rejection of claim 8 should be withdrawn.

#### Dependent Claims 9-11

Each of dependent claims 9-11 depends either directly or indirectly from claim 8, and thus inherits all limitations of claim 8. It is respectfully submitted that dependent claims 9-11 are allowable not only because of their dependency from independent claim 8 for the reasons discussed above, but also in view of their novel claim features (which both narrow the scope of the particular claims and compels a broader interpretation of claim 8).

#### **VIII. Newly Added Claim**

Claim 26 is added herein. Claim 26 depends from claim 12, and is thus believed to be allowable over the applied art for at least the reasons discussed above with claim 12.



Application No. 11/403,552

Docket No.: 69936/P003US/10601230

**IX. Conclusion**

In view of the above, Applicant believes the pending application is in condition for allowance.

Applicant believes a fee of \$50.00 for an additional claim is due with this response. However, if any additional fee is due, please charge our Deposit Account No. 06-2380, under Order No. 69936/P003US/10601230 from which the undersigned is authorized to draw.

Dated: August 19, 2008

Respectfully submitted,

By 

Jody C. Bishop

Registration No.: 44,034

FULBRIGHT & JAWORSKI L.L.P.

2200 Ross Avenue, Suite 2800

Dallas, Texas 75201-2784

(214) 855-8007

(214) 855-8200 (Fax)

Attorney for Applicant

# **EXHIBIT 8**

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with § 1.6(a)(4).

Dated: January 21, 2009

Signature: Donna Forbit

(Donna Forbit)

Docket No.: 69936/P003US/10601230  
(PATENT)

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Patent Application of:  
Christopher S. Signaoff et al.

Application No.: 11/403,552

Confirmation No.: 7846

Filed: April 13, 2006

Art Unit: 2616

For: SYSTEM AND METHOD FOR CROSS  
PROTOCOL COMMUNICATION

Examiner: T. H. Phan

**AMENDMENT IN RESPONSE TO SECOND NON-FINAL OFFICE ACTION**

MS Amendment  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Dear Sir:

**INTRODUCTORY COMMENTS**

In response to the Office Action dated December 3, 2008, Applicant respectfully requests the Examiner to reconsider and withdraw the rejections in view of the remarks contained herein.

**No Amendments to the Claims** are presented herein. For the Examiner's convenience a listing of the claims is provided beginning on page 2 of this paper.

**Remarks/Arguments** begin on page 9 of this paper.

**LISTING OF THE CLAIMS**

1. (Previously Presented) A method for multimedia communication comprising:

- receiving a multimedia data stream at a communication controller in a first protocol from a communication device, wherein the first protocol comprises a signaling protocol;
- detecting a type of said first protocol;
- converting said first protocol into an intermediate protocol;
- translating said intermediate protocol into a second protocol, wherein the second protocol comprises a signaling protocol; and
- transmitting said multimedia data stream in said second protocol to a target communication device.

2. (Previously Presented) The method of claim 1 further comprising:

- communicating, prior to said translating, said multimedia data stream in said communication controller to a second communication controller connected to said target communication device; wherein said translating and said transmitting are performed by said second communication controller.

3. (Original) The method of claim 1 wherein said converting comprises:

- accessing a first protocol table responsive to said type, wherein said first protocol table includes a plurality of first protocol messages corresponding to a plurality of intermediate protocol messages;
- selecting ones of said plurality of intermediate protocol messages that correspond to one or more first protocol messages found in said multimedia data stream; and
- assembling said ones of said plurality of intermediate protocol messages to form said multimedia data stream in said intermediate protocol.

4. (Original) The method of claim 1 wherein said translating comprises:  
determining a second protocol type associated with said target communication device;  
accessing a second protocol table responsive to said second protocol type, wherein said second protocol table includes a plurality of second protocol messages corresponding to said plurality of intermediate protocol messages;  
selecting ones of said plurality of second protocol messages that correspond to one or more intermediate protocol messages found in said multimedia data stream; and  
assembling said ones of said plurality of second protocol messages to form said multimedia data stream in said second protocol.

5. (Original) The method of claim 4 further comprising:  
retrieving said second protocol type from a device information base, wherein said device information base contains compatibility information for each device available for said multimedia communication.

6. (Original) The method of claim 1 wherein said first protocol comprises one of a text-based protocol and a binary protocol and wherein said second protocol comprises one of a binary protocol and a text-based protocol.

7. (Original) The method of claim 6 wherein said intermediate protocol comprises protocol messages common to said text-based protocol and said binary protocol.

8. (Previously Presented) A communication controller in a multimedia communication system, said communication controller comprising:

- a message interface to transceive multimedia data from a communication endpoint in a first protocol, wherein the first protocol comprises a signaling protocol;
- a protocol signaler to determine a type of said first protocol;
- a first protocol conversion table that contains a plurality of first protocol messages and a plurality of interim protocol messages, wherein said plurality of interim protocol messages correspond to ones of said plurality of first protocol messages;
- a protocol conversion utility to convert said first protocol into an interim protocol using said first protocol conversion table; and
- a network interface to transceive said multimedia data in said interim protocol to a target communication endpoint.

9. (Original) The communication controller of claim 8 wherein said protocol conversion utility converts said interim protocol of a received multimedia data stream into a second protocol and wherein said message interface transmits said received multimedia data stream in said second protocol to a destination endpoint connected to said communication controller.

10. (Original) The communication controller of claim 9 further comprising:

- a second protocol conversion table that contains a plurality of second protocol messages and said plurality of interim protocol messages, wherein said plurality of interim protocol messages correspond to ones of said plurality of second protocol messages.

11. (Original) The communication controller of claim 9 further comprising:

- an endpoint information base including compatibility data on one or more communication endpoints connected to said communication controller, wherein said compatibility data includes a device protocol type.

12. (Previously Presented) A method for multimedia communication comprising:

- receiving a multimedia data stream at a communication controller in a first protocol from a communication device;
- detecting a type of said first protocol;
- converting said first protocol into an intermediate protocol, wherein said converting is performed irrespective of a second protocol in which the multimedia data stream is to be transmitted to a target communication device;
- translating said intermediate protocol into said second protocol; and
- transmitting said multimedia data stream in said second protocol to the target communication device.

13. (Previously Presented) The method of claim 12 further comprising:

- communicating, prior to said translating, said multimedia data stream in said communication controller to a second communication controller connected to said target communication device; wherein said translating and said transmitting are performed by said second communication controller.

14. (Original) The method of claim 12 wherein said converting comprises:

- accessing a first protocol table responsive to said type, wherein said first protocol table includes a plurality of first protocol messages corresponding to a plurality of intermediate protocol messages;
- selecting ones of said plurality of intermediate protocol messages that correspond to one or more first protocol messages found in said multimedia data stream; and
- assembling said ones of said plurality of intermediate protocol messages to form said multimedia data stream in said intermediate protocol.

15. (Original) The method of claim 12 wherein said translating comprises:

- determining a second protocol type associated with said target communication device;
- accessing a second protocol table responsive to said second protocol type, wherein said second protocol table includes a plurality of second protocol messages corresponding to said plurality of intermediate protocol messages;
- selecting ones of said plurality of second protocol messages that correspond to one

or more intermediate protocol messages found in said multimedia data stream; and  
assembling said ones of said plurality of second protocol messages to form said multimedia data stream in said second protocol.

16. (Original) The method of claim 15 further comprising:  
retrieving said second protocol type from a device information base, wherein said device information base contains compatibility information for each device available for said multimedia communication.

17. (Original) The method of claim 12 wherein said first protocol comprises one of a text-based protocol and a binary protocol and wherein said second protocol comprises one of a binary protocol and a text-based protocol.

18. (Original) The method of claim 17 wherein said intermediate protocol comprises protocol messages common to said text-based protocol and said binary protocol.

19. (Previously Presented) A computer program product having a computer readable storage medium with computer program logic recorded thereon for multimedia communication, said computer program product comprising:

code for receiving a multimedia data stream at a communication controller in a first protocol from a communication device;

code for detecting a type of said first protocol;

code for converting said first protocol into an intermediate protocol, wherein said converting is performed irrespective of a second protocol in which the multimedia data stream is to be transmitted to a target communication device;

code for translating said intermediate protocol into the second protocol; and

code for transmitting said multimedia data stream in said second protocol to the target communication device.

20. (Previously Presented) The computer program product of claim 19 further comprising:

code for communicating, prior to execution of said code for translating, said multimedia data stream in said communication controller to a second communication controller connected to said target communication device; wherein said code for translating and said code for transmitting are executed at said second communication controller.



21. (Original) The computer program product of claim 19 wherein said code for converting comprises:

code for accessing a first protocol table responsive to said type, wherein said first protocol table includes a plurality of first protocol messages corresponding to a plurality of intermediate protocol messages;

code for selecting ones of said plurality of intermediate protocol messages that correspond to one or more first protocol messages found in said multimedia data stream; and

code for assembling said ones of said plurality of intermediate protocol messages to form said multimedia data stream in said intermediate protocol.

22. (Original) The computer program product of claim 19 wherein said code for translating comprises:

code for determining a second protocol type associated with said target communication device;

code for accessing a second protocol table responsive to said second protocol type, wherein said second protocol table includes a plurality of second protocol messages corresponding to said plurality of intermediate protocol messages;

code for selecting ones of said plurality of second protocol messages that correspond to one or more intermediate protocol messages found in said multimedia data stream; and

code for assembling said ones of said plurality of second protocol messages to form said multimedia data stream in said second protocol.

23. (Original) The computer program product of claim 22 further comprising:  
code for retrieving said second protocol type from a device information base, wherein said device information base contains compatibility information for each device available for said multimedia communication.

24. (Original) The computer program product of claim 19 wherein said first protocol comprises one of a text-based protocol and a binary protocol and wherein said second protocol comprises one of a binary protocol and a text-based protocol.

Application No. 11/403,552

Docket No.: 69936/P003US/10601230

25. (Original) The computer program product of claim 24 wherein said intermediate protocol comprises protocol messages common to said text-based protocol and said binary protocol.

26. (Previously Presented) The method of claim 12 wherein said first protocol comprises a signaling protocol, and wherein said second protocol comprises a signaling protocol.

## REMARKS

### **I. Overview**

Claims 1-26 were pending in this application. Applicant thanks the Examiner for reconsidering and withdrawing the objections and rejections raised in the first Office Action under 35 U.S.C. § 112, second paragraph and 35 U.S.C. § 101.

The issues raised in the second Office Action of December 3, 2008 (*Office Action*) are as follows:

- Claims 1-7 and 12-26 are rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 7,346,076 to Habiby et al.(hereinafter “*Habiby*”).
- Claims 8-11 are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,963,583 to Foti (hereinafter “*Foti*”) in view of *Habiby*.

In response, Applicant respectfully traverses all claim rejections and requests reconsideration and withdrawal in light of the remarks presented herein.

### **II. Rejections Under 35 U.S.C. §102 over *Habiby***

Claims 1-7 and 12-26 are rejected under 35 U.S.C. §102(e) as being anticipated by *Habiby*. Applicant respectfully traverses these rejections for the reasons below.

To anticipate a claim under 35 U.S.C. § 102, a single reference must teach each and every element of the claim. *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631 (Fed. Cir. 1987). In fact, “[t]he identical invention must be shown in as complete detail as is contained in the . . . claim.” *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236 (Fed. Cir. 1989). Furthermore, for a reference to be anticipatory, “[its] elements must be arranged as required by the claim.” *In re Bond*, 910 F.2d 831 (Fed. Cir. 1990), *cited in* M.P.E.P. § 2131. As discussed below, *Habiby* fails to teach all elements of claims 1-7 and 12-26, and therefore fails to anticipate the claims under 35 U.S.C. §102.

#### Independent Claim 1

Claim 1 recites, in part, “receiving a multimedia data stream at a communication controller in a first protocol from a communication device, wherein the first protocol

comprises a signaling protocol; detecting a type of said first protocol; converting said first protocol into an intermediate protocol;...” (emphasis added). As discussed in Applicant’s previous response and reiterated further below, *Habiby* fails to disclose converting a first protocol that comprises a signaling protocol into an intermediate protocol.

*Habiby* appears to generally describe use of gateways to perform bearer format conversion, enabling a call to pass between networks using different internal bearer formats, *see* col. 3, lines 34-39. In discussing its Figure 1, *Habiby* explains that the format of the bearer traffic between originating node 12 and ingress gateway 22 is “bearer format 1”; the format of the bearer traffic between ingress and egress gateways 22, 24 is “bearer format 2”; and the format of the bearer traffic between egress gateway 24 and terminating node 14 is “bearer format 3”, *see* col. 3, line 64 - col. 4, line 3.

However, *Habiby* distinguishes the “bearer traffic” from “signaling protocols”, such as H.323 and SIP. For instance, *Habiby* states that “In order for controllers 26, 28 to exchange the necessary format conversion information, standard messages found in the Bearer Independent Call Control (BICC) signaling protocol may be used”; and “Other signaling protocols, including Session Initiation Protocol (SIP), SIP-T, H.323, PNNI, and B-ISUP, may also be used.” Col. 7, lines 27-32. Thus, while *Habiby* mentions conversion of its bearer traffic, it does NOT propose any conversion of the “signaling protocol” messages. Instead, *Habiby* proposes use of such signaling protocol messages to determine the appropriate conversion of the “bearer traffic”. That is, the signaling protocol messages themselves are not converted in *Habiby*, but are instead used to exchange conversion information for converting the bearer traffic.

The current *Office Action* contends on pages 2-3 thereof that the bearer information at gateway controllers 26/28 of *Habiby* is signaling protocol, citing to col. 7, lines 27-43 of *Habiby*. However, as discussed above, at col. 7, lines 27-32 *Habiby* actually distinguishes its bearer traffic from the signaling protocols. That is, *Habiby* makes clear that the bearer traffic that it proposes converting is NOT a signaling protocol. Again, *Habiby* proposes use of signaling protocol messages to determine the appropriate conversion of the “bearer traffic”, but the signaling protocol messages themselves are not converted in *Habiby*. Instead, the signaling protocol messages of *Habiby* are used to exchange conversion information for

converting the bearer traffic. It is only the bearer traffic (which is NOT in a signaling protocol) that is converted in *Habiby*.

Thus, *Habiby* fails to teach converting a first protocol to an intermediate protocol, where the first protocol comprises a signaling protocol, as recited by claim 1. In view of the above, the rejection of claim 1 should be withdrawn.

#### Independent Claim 12

Claim 12 recites, in part, “converting said first protocol into an intermediate protocol, wherein said converting is performed irrespective of a second protocol in which the multimedia data stream is to be transmitted to a target communication device; translating said intermediate protocol into said second protocol; and transmitting said multimedia data stream in said second protocol to the target communication device” (emphasis added). As discussed in Applicant’s previous response and reiterated further below, *Habiby* fails to disclose performing its converting irrespective of a second protocol in which the multimedia data stream is to be transmitted to a target communication device. Further, in its treatment of claim 12 on pages 2-3, the current *Office Action* fails to even mention the above-emphasized limitation and thus fails to provide any indication whatsoever where such limitation is believed to be taught within the disclosure of *Habiby*.

*Habiby* appears to describe a system in which a determination is made as to whether to perform its conversion based on first determining the bearer format of a target communication device. For instance, at col. 2, line 62 – col. 3, line 5, *Habiby* explains:

To efficiently determine which, if any, bearer format conversion must occur for a particular communication channel over paths 18, 20, the gateway controllers 26, 28 determine the bearer format used at each of the nodes. If, for example, an originating node 12 uses an IP protocol and terminating node 14 uses a TDM protocol, then a conversion is performed between IP and TDM somewhere along the communication path. If the originating and terminating nodes use the same bearer format as that used by the backbone network 16, then no conversion is required or performed.

Thus, *Habiby* does NOT teach performing its “irrespective of a second protocol in which the multimedia data stream is to be transmitted to a target communication device”, but

instead expressly teaches that it determines whether to perform its conversion based on knowledge of the bearer formats of the originating and terminating nodes.

Therefore, *Habiby* fails to anticipate claim 12, and thus the rejection of claim 12 should be withdrawn.

#### Independent Claim 19

Claim 19 recites, in part, “code for converting said first protocol into an intermediate protocol, wherein said converting is performed irrespective of a second protocol in which the multimedia data stream is to be transmitted to a target communication device; code for translating said intermediate protocol into the second protocol; and code for transmitting said multimedia data stream in said second protocol to the target communication device” (emphasis added). As discussed above with claim 12, *Habiby* fails to disclose performing its converting irrespective of a second protocol in which the multimedia data stream is to be transmitted to a target communication device. Further, as with claim 12, the Office Action’s treatment of claim 19 on pages 2-3 fails to even mention the above-emphasized limitation and thus fails to provide any indication whatsoever where such limitation is believed to be taught within the disclosure of *Habiby*.

Therefore, *Habiby* fails to anticipate claim 19, and thus the rejection of claim 19 should be withdrawn.

#### Dependent Claims 2-7, 13-18, and 20-26

Each of dependent claims 2-7, 13-18, and 20-26 depends either directly or indirectly from one of independent claims 1, 12, and 19, and thus each inherits all limitations of the respective independent claim from which it depends. It is respectfully submitted that dependent claims 2-7, 13-18, and 20-26 are allowable not only because of their dependency from their respective independent claim for the reasons discussed above, but also in view of their novel claim features (which both narrow the scope of the particular claims and compels a broader interpretation of their respective independent claim).

Further, dependent claim 26 recites “wherein said first protocol comprises a signaling protocol, and wherein said second protocol comprises a signaling protocol.” For reasons

similar to those discussed above with claim 1, *Habiby* fails to teach these further limitations of claim 26. That is, *Habiby* fails to teach conversion of its signaling protocol messages, but instead merely proposes conversion of its bearer traffic, which it distinguishes from signaling protocol messages. Accordingly, the rejection of claim 26 should be withdrawn for this further reason.

### **III. Rejections Under 35 U.S.C. §103 over *Foti* in view of *Habiby***

Claims 8-11 are rejected under 35 U.S.C. §103(a) as being obvious over *Foti* in view of *Habiby*. Applicant respectfully traverses this rejection as provided further below.

The test for non-obvious subject matter is whether the differences between the subject matter and the prior art are such that the claimed subject matter as a whole would have been obvious to a person having ordinary skill in the art to which the subject matter pertains. The United States Supreme Court in Graham v. John Deere and Co., 383 U.S. 1 (1966) set forth the factual inquiries which must be considered in applying the statutory test: (1) determining of the scope and content of the prior art; (2) ascertaining the differences between the prior art and the claims at issue; and (3) resolving the level of ordinary skill in the pertinent art. As discussed further hereafter, Applicant respectfully asserts that the claims include non-obvious differences over the cited art.

As discussed further below, the rejections should be overturned because when considering the scope and content of the applied *Foti* and *Habiby* references there are significant differences between the applied combination and claims 8-11, as the applied combination fails to disclose all elements of these claims. Thus, considering the lack of disclosure in the applied combination of all elements of claims 8-11, one of ordinary skill in the art would not find these claims obvious under 35 U.S.C. §103, and therefore the rejections should be withdrawn.

Independent Claim 8

Claim 8 recites:

A communication controller in a multimedia communication system, said communication controller comprising:  
a message interface to transceive multimedia data from a communication endpoint in a first protocol, wherein the first protocol comprises a signaling protocol;  
a protocol signaler to determine a type of said first protocol;  
a first protocol conversion table that contains a plurality of first protocol messages and a plurality of interim protocol messages, wherein said plurality of interim protocol messages correspond to ones of said plurality of first protocol messages;  
a protocol conversion utility to convert said first protocol into an interim protocol using said first protocol conversion table; and  
a network interface to transceive said multimedia data in said interim protocol to a target communication endpoint. (Emphasis added).

Thus, claim 8 recites that a first protocol comprises a signaling protocol, and further recites a protocol conversion utility to convert said first protocol into an interim protocol. The applied combination of *Foti* and *Habiby* fails to teach or suggest these elements of claim 8, as discussed below.

As discussed above, *Habiby* does not teach or suggest converting a protocol that comprises a signaling protocol into an interim protocol. Instead, *Habiby* uses signaling protocol information for converting bearer traffic, but does not disclose any conversion of its signaling protocol.

*Foti*, on the other hand, appears to discuss conversion of various different signaling protocols, such as SIP and H.323, *see e.g.*, col. 1, line 5 - col. 3, line 67. However, the Examiner concedes in the Office Action that *Foti* does not disclose conversion of a first protocol into an interim protocol, *see* page 7 of the *Office Action*. The *Office Action* relies on *Habiby* as disclosing such a conversion to an interim protocol.

However, as discussed above with claim 1, *Habiby* does not propose any such conversion of its signaling protocol (but instead only uses the signaling protocol information for converting its bearer traffic). Thus, *Habiby* does not teach or suggest conversion of a



Application No. 11/403,552

Docket No.: 69936/P003US/10601230

signaling protocol at all, and *Foti* does not teach or suggest conversion of a signaling protocol to an interim protocol.

Accordingly, the applied combination of *Foti* and *Habiby* does not teach or suggest the above elements of claim 8, as neither reference teaches or suggests conversion of a protocol that comprises a signaling protocol into an interim protocol. Therefore, the rejection of claim 8 should be withdrawn.

#### Dependent Claims 9-11

Each of dependent claims 9-11 depends either directly or indirectly from claim 8, and thus inherits all limitations of claim 8. It is respectfully submitted that dependent claims 9-11 are allowable not only because of their dependency from independent claim 8 for the reasons discussed above, but also in view of their novel claim features (which both narrow the scope of the particular claims and compels a broader interpretation of claim 8).

#### **IV. Conclusion**

In view of the above, Applicant believes the pending application is in condition for allowance.

Applicant believes no fee is due with this response. However, if any additional fee is due, please charge our Deposit Account No. 06-2380, under Order No. 69936/P003US/10601230 from which the undersigned is authorized to draw.

Dated: January 21, 2009

Respectfully submitted,

By 

Jody C. Bishop

Registration No.: 44,034

FULBRIGHT & JAWORSKI L.L.P.

2200 Ross Avenue, Suite 2800

Dallas, Texas 75201-2784

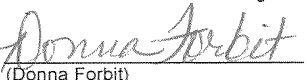
(214) 855-8007

(214) 855-8200 (Fax)

Attorney for Applicant

# **EXHIBIT 9**

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with § 1.6(a)(4).

Dated: September 18, 2009 Signature: 

(Donna Forbit)

Docket No.: 69936/P003US/10601230  
(PATENT)

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Patent Application of:  
Christopher S. Signaoff et al.

Application No.: 11/403,552

Confirmation No.: 7846

Filed: April 13, 2006

Art Unit: 2616

For: SYSTEM AND METHOD FOR CROSS  
PROTOCOL COMMUNICATION

Examiner: T. H. Phan

**AMENDMENT IN RESPONSE TO THIRD NON-FINAL OFFICE ACTION**

MS Amendment  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Dear Sir:

**INTRODUCTORY COMMENTS**

In response to the Office Action dated September 1, 2009, Applicant respectfully requests the Examiner to reconsider and withdraw the rejections in view of the remarks contained herein.

**No Amendments to the Claims** are presented herein. For the Examiner's convenience a listing of the claims is provided beginning on page 2 of this paper.

**Remarks/Arguments** begin on page 9 of this paper.

**LISTING OF THE CLAIMS**

1. (Previously Presented) A method for multimedia communication comprising:

- receiving a multimedia data stream at a communication controller in a first protocol from a communication device, wherein the first protocol comprises a signaling protocol;
- detecting a type of said first protocol;
- converting said first protocol into an intermediate protocol;
- translating said intermediate protocol into a second protocol, wherein the second protocol comprises a signaling protocol; and
- transmitting said multimedia data stream in said second protocol to a target communication device.

2. (Previously Presented) The method of claim 1 further comprising:

- communicating, prior to said translating, said multimedia data stream in said communication controller to a second communication controller connected to said target communication device; wherein said translating and said transmitting are performed by said second communication controller.

3. (Original) The method of claim 1 wherein said converting comprises:

- accessing a first protocol table responsive to said type, wherein said first protocol table includes a plurality of first protocol messages corresponding to a plurality of intermediate protocol messages;
- selecting ones of said plurality of intermediate protocol messages that correspond to one or more first protocol messages found in said multimedia data stream; and
- assembling said ones of said plurality of intermediate protocol messages to form said multimedia data stream in said intermediate protocol.

4. (Original) The method of claim 1 wherein said translating comprises:  
determining a second protocol type associated with said target communication device;

accessing a second protocol table responsive to said second protocol type, wherein said second protocol table includes a plurality of second protocol messages corresponding to said plurality of intermediate protocol messages;

selecting ones of said plurality of second protocol messages that correspond to one or more intermediate protocol messages found in said multimedia data stream; and

assembling said ones of said plurality of second protocol messages to form said multimedia data stream in said second protocol.

5. (Original) The method of claim 4 further comprising:

retrieving said second protocol type from a device information base, wherein said device information base contains compatibility information for each device available for said multimedia communication.

6. (Original) The method of claim 1 wherein said first protocol comprises one of a text-based protocol and a binary protocol and wherein said second protocol comprises one of a binary protocol and a text-based protocol.

7. (Original) The method of claim 6 wherein said intermediate protocol comprises protocol messages common to said text-based protocol and said binary protocol.

8. (Previously Presented) A communication controller in a multimedia communication system, said communication controller comprising:

- a message interface to transceive multimedia data from a communication endpoint in a first protocol, wherein the first protocol comprises a signaling protocol;
- a protocol signaler to determine a type of said first protocol;
- a first protocol conversion table that contains a plurality of first protocol messages and a plurality of interim protocol messages, wherein said plurality of interim protocol messages correspond to ones of said plurality of first protocol messages;
- a protocol conversion utility to convert said first protocol into an interim protocol using said first protocol conversion table; and
- a network interface to transceive said multimedia data in said interim protocol to a target communication endpoint.

9. (Original) The communication controller of claim 8 wherein said protocol conversion utility converts said interim protocol of a received multimedia data stream into a second protocol and wherein said message interface transmits said received multimedia data stream in said second protocol to a destination endpoint connected to said communication controller.

10. (Original) The communication controller of claim 9 further comprising:

- a second protocol conversion table that contains a plurality of second protocol messages and said plurality of interim protocol messages, wherein said plurality of interim protocol messages correspond to ones of said plurality of second protocol messages.

11. (Original) The communication controller of claim 9 further comprising:

- an endpoint information base including compatibility data on one or more communication endpoints connected to said communication controller, wherein said compatibility data includes a device protocol type.

12. (Previously Presented) A method for multimedia communication comprising:

receiving a multimedia data stream at a communication controller in a first protocol from a communication device;

detecting a type of said first protocol;

converting said first protocol into an intermediate protocol, wherein said converting is performed irrespective of a second protocol in which the multimedia data stream is to be transmitted to a target communication device;

translating said intermediate protocol into said second protocol; and

transmitting said multimedia data stream in said second protocol to the target communication device.

13. (Previously Presented) The method of claim 12 further comprising:

communicating, prior to said translating, said multimedia data stream in said communication controller to a second communication controller connected to said target communication device; wherein said translating and said transmitting are performed by said second communication controller.

14. (Original) The method of claim 12 wherein said converting comprises:

accessing a first protocol table responsive to said type, wherein said first protocol table includes a plurality of first protocol messages corresponding to a plurality of intermediate protocol messages;

selecting ones of said plurality of intermediate protocol messages that correspond to one or more first protocol messages found in said multimedia data stream; and

assembling said ones of said plurality of intermediate protocol messages to form said multimedia data stream in said intermediate protocol.

15. (Original) The method of claim 12 wherein said translating comprises:

determining a second protocol type associated with said target communication device;

accessing a second protocol table responsive to said second protocol type, wherein said second protocol table includes a plurality of second protocol messages corresponding to said plurality of intermediate protocol messages;

selecting ones of said plurality of second protocol messages that correspond to one

or more intermediate protocol messages found in said multimedia data stream; and  
assembling said ones of said plurality of second protocol messages to form said multimedia data stream in said second protocol.

16. (Original) The method of claim 15 further comprising:  
retrieving said second protocol type from a device information base, wherein said device information base contains compatibility information for each device available for said multimedia communication.

17. (Original) The method of claim 12 wherein said first protocol comprises one of a text-based protocol and a binary protocol and wherein said second protocol comprises one of a binary protocol and a text-based protocol.

18. (Original) The method of claim 17 wherein said intermediate protocol comprises protocol messages common to said text-based protocol and said binary protocol.

19. (Previously Presented) A computer program product having a computer readable storage medium with computer program logic recorded thereon for multimedia communication, said computer program product comprising:

code for receiving a multimedia data stream at a communication controller in a first protocol from a communication device;

code for detecting a type of said first protocol;

code for converting said first protocol into an intermediate protocol, wherein said converting is performed irrespective of a second protocol in which the multimedia data stream is to be transmitted to a target communication device;

code for translating said intermediate protocol into the second protocol; and

code for transmitting said multimedia data stream in said second protocol to the target communication device.

20. (Previously Presented) The computer program product of claim 19 further comprising:

code for communicating, prior to execution of said code for translating, said multimedia data stream in said communication controller to a second communication controller connected to said target communication device; wherein said code for translating and said code for transmitting are executed at said second communication controller.



21. (Original) The computer program product of claim 19 wherein said code for converting comprises:

code for accessing a first protocol table responsive to said type, wherein said first protocol table includes a plurality of first protocol messages corresponding to a plurality of intermediate protocol messages;

code for selecting ones of said plurality of intermediate protocol messages that correspond to one or more first protocol messages found in said multimedia data stream; and

code for assembling said ones of said plurality of intermediate protocol messages to form said multimedia data stream in said intermediate protocol.

22. (Original) The computer program product of claim 19 wherein said code for translating comprises:

code for determining a second protocol type associated with said target communication device;

code for accessing a second protocol table responsive to said second protocol type, wherein said second protocol table includes a plurality of second protocol messages corresponding to said plurality of intermediate protocol messages;

code for selecting ones of said plurality of second protocol messages that correspond to one or more intermediate protocol messages found in said multimedia data stream; and

code for assembling said ones of said plurality of second protocol messages to form said multimedia data stream in said second protocol.

23. (Original) The computer program product of claim 22 further comprising:  
code for retrieving said second protocol type from a device information base, wherein said device information base contains compatibility information for each device available for said multimedia communication.

24. (Original) The computer program product of claim 19 wherein said first protocol comprises one of a text-based protocol and a binary protocol and wherein said second protocol comprises one of a binary protocol and a text-based protocol.

Application No. 11/403,552

Docket No.: 69936/P003US/10601230

25. (Original) The computer program product of claim 24 wherein said intermediate protocol comprises protocol messages common to said text-based protocol and said binary protocol.

26. (Previously Presented) The method of claim 12 wherein said first protocol comprises a signaling protocol, and wherein said second protocol comprises a signaling protocol.

## REMARKS

### **I. Overview**

Claims 1-26 were pending in this application. In response to the Notice of Appeal and Pre-Appeal Brief Request for Review filed May 12, 2009, a Panel Decision (mailed June 18, 2009) withdrew the rejections previously maintained in the Final Office Action of April 16, 2009. Now, a third non-final Office Action dated September 1, 2009 (*Office Action*) is received. The issues raised in the third non-final *Office Action* are as follows:

- Claims 1-26 are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent Application Publication No. 2005/0125696 to Afshar (hereinafter “*Afshar*”) in view of U.S. Patent No. 6,963,583 to Foti (hereinafter “*Foti*”).

In response, Applicant respectfully traverses all claim rejections and requests reconsideration and withdrawal in light of the remarks presented herein.

### **II. Rejections Under 35 U.S.C. §103 over *Afshar* in view of *Foti***

Claims 1-26 are rejected under 35 U.S.C. §103(a) as being unpatentable over *Afshar* in view of *Foti*. Applicant respectfully traverses these rejections for the reasons below.

The test for non-obvious subject matter is whether the differences between the subject matter and the prior art are such that the claimed subject matter as a whole would have been obvious to a person having ordinary skill in the art to which the subject matter pertains. The United States Supreme Court in Graham v. John Deere and Co., 383 U.S. 1 (1966) set forth the factual inquiries which must be considered in applying the statutory test: (1) determining of the scope and content of the prior art; (2) ascertaining the differences between the prior art and the claims at issue; and (3) resolving the level of ordinary skill in the pertinent art. As discussed further hereafter, Applicant respectfully asserts that the claims include non-obvious differences over the cited art.

As discussed further below, the rejections should be withdrawn because when considering the scope and content of the applied *Afshar* and *Foti* references there are significant differences between the applied combination and claims 1-26, as the applied combination fails to teach or suggest all limitations of these claims. Thus, considering the lack of teaching or suggestion in the applied combination of all limitations of claims 1-26,

one of ordinary skill in the art would not find these claims obvious under 35 U.S.C. §103, and therefore the rejections should be withdrawn.

### **Discussion of Applied *Afshar* and *Foti* References**

Before addressing the specific claim rejections raised in the Office Action, Applicant briefly addresses the disclosure of the applied *Afshar* and *Foti* references for the convenience of the Examiner.

#### ***Afshar***

*Afshar* recognizes that “there is a need to permit SIP networks to coexist with more traditional networks, such as circuit-switched networks, and/or IP networks operating with a different protocol.” *Afshar*, ¶ 0005. “To address this need, some IP telecommunications networks rely on nodes referred to herein as border elements (BEs) to provide an interface between a customer’s premises into the VoIP network infrastructure.” *Afshar*, ¶ 0006. The BEs are “used to translate between the protocol of a customer network and the SIP protocol used by the VoIP network”. *Id.*

Figure 1 of *Afshar* shows an IP-based telecommunication network (e.g., VoIP network) 101 and a customer network (e.g., IP network) 107. A BE (104) is included in IP-based telecommunication network (101), wherein the BE (104) is an interface node located at the border of the VoIP network (101) and serves to translate between different communication protocols. For instance, it “may be necessary to interface network 101 with many different customer networks using many different communication protocols, such as SIP, H.323, TDM, and/or any other protocol.” *Afshar*, ¶ 0017. BE (104) is implemented to perform such translation between a protocol of network 101 and a protocol of customer network 107. Figure 1 of *Afshar* is further described at ¶¶ 0016-0022.

The inventors in *Afshar* recognize “that it may be advantageous in many applications to separate one or more elements of a traditional H.323 border element into separate functional entities to create what is referred to herein as a decomposed H.323 border element.” *Afshar*, ¶ 0023. As discussed further in *Afshar* (see e.g., ¶¶ 0007-0008), it proposes “a decentralized, or decomposed, H.323 BE that is useful for providing an entry

point from one or more H.323-based networks into a SIP-based VoIP network.” *Afshar*, ¶ 0008. *Afshar* proposes, for example, to decompose a H.323 BE into separate functional entities, such as a signaling entity, a media control entity, and a security element, *see e.g.*, *Afshar*, ¶ 0008 and Figures 2-4.

As will be discussed further hereafter, *Afshar* does not teach or suggest converting a first protocol into an intermediate protocol, or translating the intermediate protocol into a second protocol. Instead, *Afshar* merely teaches that its BE translates from a first communication protocol of one network (e.g., H.323) to a second communication protocol of another network (e.g., SIP), without teaching or suggesting any use whatsoever of any intermediate protocol.

*Afshar* appears to mention that certain data may be communicated (e.g., to the media or security entities) via an IP or RTP (streaming) protocol. However, contrary to the contention in the current *Office Action* (at page 3 thereof), *Afshar* does not teach or suggest converting a signaling protocol into an intermediate protocol, nor does *Afshar* teach or suggest translating such an intermediate protocol into a second protocol.

### *Foti*

Similarly, *Foti* appears to discuss conversion of various different signaling protocols, such as SIP and H.323, *see e.g.*, col. 1, line 5 - col. 3, line 67. However, *Foti* also does not teach or suggest conversion of a first protocol into an intermediate protocol, or translating the intermediate protocol into a second protocol. Indeed, the Examiner has conceded in the *Office Action* of December 3, 2008 that *Foti* does not disclose conversion of a first protocol into an interim protocol, *see* page 7 of the December 3, 2008 *Office Action* (and that *Office Action* instead relied upon another reference, *Habiby*, as purportedly disclosing such a conversion to an interim protocol).

Independent Claim 1

Claim 1 recites:

A method for multimedia communication comprising:  
receiving a multimedia data stream at a communication controller in a first protocol from a communication device, wherein the first protocol comprises a signaling protocol;  
detecting a type of said first protocol;  
converting said first protocol into an intermediate protocol;  
translating said intermediate protocol into a second protocol, wherein the second protocol comprises a signaling protocol; and  
transmitting said multimedia data stream in said second protocol to a target communication device. (Emphasis added).

The applied combination of *Afshar* and *Foti* fails to teach or suggest any such converting of a first protocol into an intermediate protocol, and translating said intermediate protocol into a second protocol, as discussed below.

First, *Foti* is not relied upon as teaching or suggesting this limitation, and indeed the Examiner has conceded in the Office Action of December 3, 2008 that *Foti* does not disclose this limitation, *see* page 7 of the December 3, 2008 Office Action.

*Afshar* likewise does not teach or suggest converting a first protocol into an intermediate protocol, or translating the intermediate protocol into a second protocol. Instead, *Afshar* merely teaches that its BE translates from a first communication protocol of one network (e.g., H.323) to a second communication protocol of another network (e.g., SIP), without teaching or suggesting any use whatsoever of any intermediate protocol.

The current *Office Action* appears to contend (on page 3 thereof) that *Afshar* discloses such an intermediate protocol at its paragraphs 0020 and 0024-0027. However, this assertion is incorrect. As discussed above, *Afshar* proposes to decompose a H.323 BE into separate functional entities, such as a signaling entity (e.g., signaling entity 201 of Figures 2-4), a media control entity (e.g., media entities 202, 301-303, and 401 of Figures 2-4), and a security element (e.g., IP FW/NAT 402 of Figure 4), *see e.g., Afshar*, ¶ 0008 and discussion of Figures 2-4. *Afshar* describes that information in a signaling protocol is communicated to the signaling entity 201, and *Afshar* appears to mention that certain other data (e.g., the payload or “media” data, as opposed to the signaling information) may be communicated

(e.g., to the media or security entities) via an IP or RTP (streaming) protocol. However, contrary to the contention in the current *Office Action* (at page 3 thereof), *Afshar* does not teach or suggest converting a signaling protocol into an intermediate protocol, nor does *Afshar* teach or suggest translating such an intermediate protocol into a second protocol. Again, any mention of converting or translating the H.323 signaling protocol in *Afshar* proposes to translate H.323 messages to SIP messages and vice versa, *see e.g., Afshar*, ¶ 0027.

Accordingly, the applied combination of *Afshar* and *Foti* does not teach or suggest at least the above limitations of claim 1, as neither reference teaches or suggests conversion of a protocol that comprises a signaling protocol into an intermediate protocol. Therefore, the rejection of claim 1 should be withdrawn.

#### Independent Claim 8

Claim 8 recites:

A communication controller in a multimedia communication system, said communication controller comprising:  
a message interface to transceive multimedia data from a communication endpoint in a first protocol, wherein the first protocol comprises a signaling protocol;  
a protocol signaler to determine a type of said first protocol;  
a first protocol conversion table that contains a plurality of first protocol messages and a plurality of interim protocol messages, wherein said plurality of interim protocol messages correspond to ones of said plurality of first protocol messages;  
a protocol conversion utility to convert said first protocol into an interim protocol using said first protocol conversion table; and  
a network interface to transceive said multimedia data in said interim protocol to a target communication endpoint. (Emphasis added).

Thus, claim 8 recites a first protocol conversion table that contains a plurality of interim protocol messages, and further recites a protocol conversion utility to convert said first protocol into an interim protocol. The applied combination of *Afshar* and *Foti* fails to teach or suggest at least these limitations of claim 8. As discussed above with claim 1, neither *Afshar* nor *Foti* teaches or suggests conversion of a signaling protocol into any interim protocol. Accordingly, the applied combination of *Afshar* and *Foti* does not teach or suggest at least the above-emphasized limitations of claim 8, as neither reference teaches or

suggests conversion of a protocol that comprises a signaling protocol into an interim protocol. Therefore, the rejection of claim 8 should be withdrawn.

Independent Claim 12

Claim 12 recites:

A method for multimedia communication comprising:  
receiving a multimedia data stream at a communication controller in a first protocol from a communication device;  
detecting a type of said first protocol;  
converting said first protocol into an intermediate protocol, wherein said converting is performed irrespective of a second protocol in which the multimedia data stream is to be transmitted to a target communication device;  
translating said intermediate protocol into said second protocol; and  
transmitting said multimedia data stream in said second protocol to the target communication device. (Emphasis added).

For reasons similar to those discussed above with claim 1, the applied combination of *Afshar* and *Foti* fails to teach or suggest at least the above-emphasized limitations of claim 12. As discussed above with claim 1, neither *Afshar* nor *Foti* teaches or suggests conversion of a first protocol into any intermediate protocol, nor do the references teach or suggest translating such intermediate protocol into a second protocol. Therefore, the rejection of claim 12 should be withdrawn.



Independent Claim 19

Claim 19 recites:

A computer program product having a computer readable storage medium with computer program logic recorded thereon for multimedia communication, said computer program product comprising:  
code for receiving a multimedia data stream at a communication controller in a first protocol from a communication device;  
code for detecting a type of said first protocol;  
code for converting said first protocol into an intermediate protocol,  
wherein said converting is performed irrespective of a second protocol in which the multimedia data stream is to be transmitted to a target communication device;  
code for translating said intermediate protocol into the second protocol; and  
code for transmitting said multimedia data stream in said second protocol to the target communication device. (Emphasis added).

For reasons similar to those discussed above with claim 1, the applied combination of *Afshar* and *Foti* fails to teach or suggest at least the above-emphasized limitations of claim 19. As discussed above with claim 1, neither *Afshar* nor *Foti* teaches or suggests conversion of a first protocol into any intermediate protocol, nor do the references teach or suggest translating such intermediate protocol into a second protocol. Therefore, the rejection of claim 19 should be withdrawn.

Dependent Claims 2-7, 9-11, 13-18, and 20-26

Each of dependent claims 2-7, 9-11, 13-18, and 20-26 depends either directly or indirectly from one of independent claims 1, 8, 12, and 19, and thus each inherits all limitations of the respective independent claim from which it depends. It is respectfully submitted that dependent claims 2-7, 9-11, 13-18, and 20-26 are allowable not only because of their dependency from their respective independent claim for the reasons discussed above, but also in view of their novel claim features (which both narrow the scope of the particular claims and compels a broader interpretation of their respective independent claim).

Application No. 11/403,552

Docket No.: 69936/P003US/10601230

### III. Conclusion

In view of the above, Applicant believes the pending application is in condition for allowance.

Applicant believes no fee is due with this response. However, if any additional fee is due, please charge our Deposit Account No. 06-2380, under Order No. 69936/P003US/10601230 from which the undersigned is authorized to draw.

Dated: September 18, 2009

Respectfully submitted,

By 

Jody C. Bishop

Registration No.: 44,034

FULBRIGHT & JAWORSKI L.L.P.

2200 Ross Avenue, Suite 2800

Dallas, Texas 75201-2784

(214) 855-8007


(214) 855-8200 (Fax)

Attorney for Applicant

# **EXHIBIT 10**

**Appeal Brief**

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with § 1.6(a)(4).

Dated: May 26, 2010 Signature: 

(Donna Forbit)

Docket No.: 69936/P002US/10601229  
(PATENT)

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Patent Application of:  
Christopher S. Signaoff et al.

Application No.: 11/403,548

Confirmation No.: 7833

Filed: April 13, 2006

Art Unit: 2437

For: SYSTEM AND METHOD FOR A  
COMMUNICATION SYSTEM

Examiner: Popham, Jeffrey D.

**APPEAL BRIEF**

MS Appeal Brief - Patents  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Dear Sir:

This brief is filed in accordance with 37 C.F.R. § 41.37(a) within one month of the Notice of Panel Decision from Pre-Appeal Brief Review, dated May 13, 2010, and is in furtherance of the Notice of Appeal filed March 23, 2010.

The fees required under 37 C.F.R. § 41.20(b)(2) for this Appeal Brief are addressed in the accompanying fee transmittal.

This brief contains items under the following headings as required by 37 C.F.R. § 41.37 and M.P.E.P. § 1206:

- I. Real Party In Interest
- II. Related Appeals and Interferences
- III. Status of Claims
- IV. Status of Amendments
- V. Summary of Claimed Subject Matter
- VI. Grounds of Rejection to be Reviewed on Appeal
- VII. Argument
- VIII. Claims Appendix
- IX. Evidence Appendix
- X. Related Proceedings Appendix

Application No. 11/403,548

Docket No.: 69936/P002US/10601229

I. REAL PARTY IN INTEREST

The real party in interest for this appeal is:

DirectPacket Research, Inc.

II. RELATED APPEALS, INTERFERENCES, AND JUDICIAL PROCEEDINGS

Appellant is aware of no appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

A. Total Number of Claims in Application

There are 23 claims pending in application, numbered 1-23.

B. Current Status of Claims

1. Claims canceled: None
2. Claims withdrawn from consideration but not canceled: None
3. Claims pending: 1-23
4. Claims allowed: None
5. Claims rejected: 1-23

C. Claims On Appeal

The claims on appeal are claims 1-23.

#### IV. STATUS OF AMENDMENTS

A Final Office Action was mailed January 29, 2010 (“the *Final Office Action*”), which finally rejected claims 1-23. In response, Applicant filed an amendment dated February 24, 2010 that presented amendments to claims 9, 16, 17, and 19. An Advisory Action was then mailed March 10, 2010 (“the *Advisory Action*”), which maintained the rejections and indicated that the amendments would be entered for purposes of appeal. In response to the *Advisory Action*, Applicant filed a Notice of Appeal with an accompanying Pre-Appeal Brief Request for Review on March 23, 2010.

A panel decision dated May 13, 2010 indicated that there is at least one actual issue for appeal, and therefore decided that the appeal should proceed to the Board. Therefore, Appellant respectfully submits this Appeal Brief in furtherance of the appeal.

Accordingly, because the claim amendments to claims 9, 16, 17, and 19 presented in the after-final response dated February 24, 2010 were indicated in the *Advisory Action* as being entered for purposes of appeal, the claims on appeal are those as amended in the February 24, 2010 amendment. A complete listing of the claims is provided in the Claims Appendix hereto.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The following provides a concise explanation of the subject matter defined in each of the separately argued claims involved in the appeal, referring to the specification by page and line number and to the drawings by reference characters, as required by 37 C.F.R. § 41.37(c)(1)(v). Each element of the claims is identified by a corresponding reference to the specification and drawings where applicable. It should be noted that the citation to passages in the specification and drawings for each claim element does not imply that the limitations from the specification and drawings should be read into the corresponding claim element.

According to one claimed embodiment, such as that of independent claim 1, a method for a multimedia communication is provided. The method comprises:

receiving, at a controller (e.g., back end controller 407 of FIG. 4) that is behind a firewall (e.g., firewall 409 of FIG. 4) and that is communicatively coupled with a plurality of endpoint communication devices (e.g., endpoint communication devices 403-406 of FIG. 4), a plurality of multiport packets of data in a multiport communication protocol for communication from at least one of the plurality of endpoint communication devices;

converting, by said controller (e.g., back end controller 407 of FIG. 4), said plurality of multiport packets into a plurality of single-port packets in a single-port communication protocol;

receiving (e.g., operational block 600 of FIG. 6) at an external controller (e.g., front end controller 410 of FIG. 4) a communication request from said controller behind said firewall (e.g., back end controller 407 of FIG. 4), wherein said external controller (e.g., front end controller 410 of FIG. 4) is not behind said firewall (e.g., firewall 409 of FIG. 4);

establishing (e.g., operational block 601 of FIG. 6) a communication channel between said controller (e.g., back end controller 407 of FIG. 4) and said external controller (e.g., front end controller 410 of FIG. 4);

opening (e.g., operational block 602 of FIG. 6) a second communication channel between said external controller (e.g., front end controller 410 of FIG. 4) and at least one other controller (e.g., back end controller 420 of FIG. 4) behind another firewall (e.g., firewall 418 of FIG. 4), wherein said at least one other controller is configured to service a single endpoint communication device (e.g., device 419 of FIG. 4);

transmitting (e.g., operational block 603 of FIG. 6) multimedia communication data between said controller (e.g., back end controller 407 of FIG. 4) and said at least one other controller (e.g., back end controller 420 of FIG. 4) wherein said multimedia communication data passes through said

external controller (e.g., front end controller 410 of FIG. 4); and

distributing (e.g., operational block 604 of FIG. 6) said multimedia communication data to one or more of said plurality of endpoint communication devices (e.g., endpoint communication devices 403-406 of FIG. 4) and said single endpoint communication device (e.g., device 419 of FIG. 4), and *see e.g.*, paragraphs 0032-0038 at page 10, line 1 – page 12, line 14 and paragraph 0043 at page 14, lines 1-11 of the specification.

In certain embodiments, such as that of dependent claim 6, the method further comprises:

issuing a central request from said external controller (e.g., front end controller 806 of FIG. 8) to a central controller (e.g., super front end controller 800 of FIG. 8) responsive to said communication request requesting to communicate with an external endpoint device (e.g., endpoint device 818 of FIG. 8) not connected to one or more of said controller and said at least one other controller; and

receiving said multimedia communication data at said central controller, and *see e.g.*, paragraphs 0045-0048 at page 14, line 25 – page 16, line 8 of the specification.

In certain embodiments, such as that of dependent claim 7, the method further comprises:

determining a peripheral controller (e.g., front end controller 804 of FIG. 8) connected to said external endpoint device (e.g., endpoint device 818 of FIG. 8);

opening another external channel between said central controller (e.g., front end controller 800 of FIG. 8) and said peripheral controller (e.g., front end controller 804 of FIG. 8);

forwarding said multimedia communication data to said peripheral controller (e.g., front end controller 804 of FIG. 8) from said central controller (e.g., front end controller 800 of FIG. 8); and

distributing said multimedia communication data to said external endpoint device (e.g., endpoint device 818 of FIG. 8), and *see e.g.*, paragraphs 0045-0048 at page 14, line 25 – page 16, line 8 of the specification.

In certain embodiments, such as that of dependent claim 8, the method further comprises:

distributing said multimedia communication data to said external endpoint device (e.g., endpoint device 818 of FIG. 8) when said external endpoint device is connected to said central controller (e.g., front end controller 800 of FIG. 8), and *see e.g.*, paragraphs 0045-0048 at page 14, line 25 – page 16, line 8 of the specification.

According to another claimed embodiment, such as that of independent claim 9, a communication community is provided. The communication community comprises:



one or more shared controllers (e.g., back end controller 407 of FIG. 4) connected to one or more endpoint communication devices (e.g., devices 403-406 of FIG. 4), wherein said one or more shared controllers is behind a firewall (e.g., firewall 409 of FIG. 4), and wherein said one or more shared controllers is operable to convert a plurality of multiport packets received from said one or more endpoint communication devices into a plurality of single-port packets in a single-port communication protocol;

at least one individual controller (e.g., back end controller 420 of FIG. 4) connected to a single endpoint communication device (e.g., device 419 of FIG. 4), wherein said at least one individual controller is behind another firewall (e.g., firewall 418 of FIG. 4), and wherein said at least one individual controller is operable to reconvert said plurality of single-port packets into said multiport communication protocol, resulting in reconverted plurality of multiport packets, and transmit to said single endpoint communication device said reconverted plurality of multiport packets using two or more ports associated with said multiport communication protocol; and

an external controller (e.g., front end controller 410 of FIG. 4) that comprises a device, said external controller in connection to said one or more shared controllers (e.g., back end controller 407 of FIG. 4) and said at least one individual controller (e.g., back end controller 420 of FIG. 4), wherein said external controller is not behind said firewall (e.g., firewall 409 of FIG. 4) or said another firewall (e.g., firewall 418 of FIG. 4), and wherein said external controller facilitates communication between ones of said one or more endpoint communication devices (e.g., devices 403-406 of FIG. 4) and said single endpoint communication device (e.g., device 419 of FIG. 4), and *see e.g.*, paragraphs 0032-0038 at page 10, line 1 – page 12, line 14 and paragraph 0043 at page 14, lines 1-11 of the specification.

According to another claimed embodiment, such as that of independent claim 14, a method for communicating is provided. The method comprises:

establishing (e.g., operational block 700 of FIG. 7) a first communication connection between a first internal controller (e.g., back end controller 808 of FIG. 8) behind a firewall and a first external controller (e.g., front end controller 806 of FIG. 8) in a first communication community (e.g., community 82 of FIG. 8), said first external controller not behind said firewall, wherein a first communication request is initiated by a local communication device (e.g., device 816 of FIG. 8) connected to the first internal controller;

establishing (e.g., operational block 701 of FIG. 7) a second communication connection between a second internal controller (e.g., back end controller 811 of FIG. 8) behind a second

firewall and a second external controller (e.g., front end controller 804 of FIG. 8) in a second communication community (e.g., community 83 of FIG. 8), said second external controller not behind said second firewall, wherein a second communication request is initiated by a remote communication device (e.g., device 818 of FIG. 8) connected to the second internal controller;

responsive to one or more of the first and second communication request requesting communication between the local communication device (e.g., device 816 of FIG. 8) and the remote communication device (e.g., device 818 of FIG. 8), establishing (e.g., operational block 702 of FIG. 7) a third communication connection between the first and second external communication controllers (e.g., controllers 806 and 804 of FIG. 8); and

transmitting (e.g., operational block 703 of FIG. 7) communication data between the first and second communication communities through the third communication connection, wherein said transmitting comprises:

receiving, at a first intermediate communication device (e.g., back end controller 808 of FIG. 8) that is behind said firewall a plurality of multiport packets of data in a multiport communication protocol for communication from said local communication device (e.g., device 816 of FIG. 8) in said first communication community (e.g., community 82 of FIG. 8),

converting, by said first intermediate communication device (e.g., back end controller 808 of FIG. 8), said plurality of multiport packets into a plurality of single-port packets in a single-port communication protocol,

transmitting, through the third communication connection, said plurality of single-port packets to a second intermediate communication device (e.g., back end controller 804 of FIG. 8) that is behind said second firewall,

receiving said plurality of single-port packets at said second intermediate communication device (e.g., back end controller 804 of FIG. 8),

reconverting, by said second intermediate communication device (e.g., back end controller 804 of FIG. 8), said received plurality of single-port packets into said multiport communication protocol, resulting in reconverted plurality of multiport packets, and

delivering, from said second intermediate communication device (e.g., back end controller 804 of FIG. 8) to said remote communication device (e.g., device 818 of FIG. 8) in said second communication community (e.g., community 83 of FIG. 8), said reconverted plurality of multiport packets using two or more ports associated with said multiport communication protocol, and *see e.g.*, paragraphs 0044-0049 at page 14, line 12 – page 16, line 14 of the specification.

In certain embodiments, such as that of dependent claim 17, the establishing a third communication connection comprises:

issuing a third communication request to a central communication controller (e.g., super front end controller 800 of FIG. 8);

establishing a first central communication channel between said first external controller (e.g., front end controller 806 of FIG. 8) and said central communication controller (e.g., front end controller 800 of FIG. 8);

issuing a fourth communication request from said central communication controller (e.g., front end controller 800 of FIG. 8) to said second external controller (e.g., front end controller 804 of FIG. 8); and

establishing a second central communication channel between said central communication controller (e.g., front end controller 800 of FIG. 8) and said second external controller (e.g., front end controller 804 of FIG. 8), and *see e.g.*, paragraphs 0044-0049 at page 14, line 12 – page 16, line 14 of the specification.

In certain embodiments, such as that of dependent claim 18, the method further comprises:

verifying said third communication request at said central communication controller (e.g., front end controller 800 of FIG. 8) prior to said establishing said first central communication channel;

verifying said fourth communication request prior to said establishing said second central communication channel, and *see e.g.*, paragraphs 0044-0049 at page 14, line 12 – page 16, line 14 of the specification.

Application No. 11/403,548

Docket No.: 69936/P002US/10601229

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Claims 14-16, 22, and 23 are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent Application Publication No. 2007/0036143 to Alt (hereinafter “*Alt*”) in view of U.S. Patent Application Publication No. 2005/0080919 to Li (hereinafter “*Li*”);

B. Claims 1-5 and 9-13, and 19-21 are rejected under 35 U.S.C. § 103(a) as being unpatentable over *Alt* in view of U.S. Patent Application Publication No. 2003/0065737 to Aasman (hereinafter “*Aasman*”) and further in view of *Li*;

C. Claims 17 and 18 are rejected under 35 U.S.C. § 103(a) as being unpatentable over *Alt* in view of *Li* and further in view of U.S. Patent Application Publication No. 2005/0122964 to Strathmeyer (hereinafter “*Strathmeyer*”); and

D. Claims 6-8 are rejected under 35 U.S.C. § 103(a) as being unpatentable over *Alt* in view of *Aasman* and *Li* and further in view of *Strathmeyer*.

## VII. ARGUMENT

Appellant respectfully traverses the outstanding rejections of the pending claims, and requests that the Board reverse the outstanding rejections in light of the remarks contained herein. The claims do not stand or fall together. Instead, Appellant presents separate arguments for various independent and dependent claims. Each of these arguments is separately argued below and presented with separate headings and sub-heading as required by 37 C.F.R. § 41.37(c)(1)(vii).

### A. Rejections Under 35 U.S.C. §103 over *Alt* in view of *Li*

Claims 14-16, 22, and 23 are rejected under 35 U.S.C. § 103(a) as being unpatentable over *Alt* in view of *Li*. Appellant respectfully traverses these rejections for the reasons below.

The test for non-obvious subject matter is whether the differences between the subject matter and the prior art are such that the claimed subject matter as a whole would have been obvious to a person having ordinary skill in the art to which the subject matter pertains. The United States Supreme Court in Graham v. John Deere and Co., 383 U.S. 1 (1966) set forth the factual inquiries which must be considered in applying the statutory test: (1) determining of the scope and content of the prior art; (2) ascertaining the differences between the prior art and the claims at issue; and (3) resolving the level of ordinary skill in the pertinent art. As discussed further hereafter, Appellant respectfully asserts that the claims include non-obvious differences over the cited art.

As discussed further below, the rejections should be overturned because when considering the scope and content of the applied *Alt* and *Li* references there are significant differences between the applied combination and claims 14-16, 22, and 23, as the applied combination fails to teach or suggest all limitations of these claims. Thus, considering the lack of teaching or suggestion in the applied combination of all limitations of claims 14-16, 22, and 23, one of ordinary skill in the art would not find these claims obvious under 35 U.S.C. §103, and therefore the rejections should be overturned.

**Independent Claim 14 and Dependent Claims 15-16, 22, and 23**

Claim 14 recites:

A method for communicating comprising:

- establishing a first communication connection between a first internal controller behind a firewall and a first external controller in a first communication community, said first external controller not behind said firewall, wherein a first communication request is initiated by a local communication device connected to the first internal controller;
- establishing a second communication connection between a second internal controller behind a second firewall and a second external controller in a second communication community, said second external controller not behind said second firewall, wherein a second communication request is initiated by a remote communication device connected to the second internal controller;
- responsive to one or more of the first and second communication request requesting communication between the local communication device and the remote communication device, establishing a third communication connection between the first and second external communication controllers; and
- transmitting communication data between the first and second communication communities through the third communication connection, wherein said transmitting comprises:
  - receiving, at a first intermediate communication device that is behind said firewall a plurality of multiport packets of data in a multiport communication protocol for communication from said local communication device in said first communication community,
  - converting, by said first intermediate communication device, said plurality of multiport packets into a plurality of single-port packets in a single-port communication protocol,
  - transmitting, through the third communication connection, said plurality of single-port packets to a second intermediate communication device that is behind said second firewall,
  - receiving said plurality of single-port packets at said second intermediate communication device,
  - reconverting, by said second intermediate communication device, said received plurality of single-port packets into said multiport communication protocol, resulting in reconverted plurality of multiport packets, and
  - delivering, from said second intermediate communication device to said remote communication device in said second communication community, said reconverted plurality of multiport packets using two or more ports associated with said multiport communication protocol. (Emphasis added).

The Examiner contends in the *Advisory Action* that *Alt* is merely relied upon for its disclosure of NAT devices that can translate ports/addresses of multiport packets. The Examiner concedes that *Alt* does not teach or suggest any conversion of multiport packets into single-port packets, nor does it teach or suggest any reversion of single-port packets to multiport packets. Instead, the Examiner relies upon *Li* as disclosing such conversion and reversion.

Thus, the Examiner contends that *Li* discloses conversion and reversion, and *Alt* discloses where such conversion and reversion may be performed (i.e., at its NAT devices), *see* page 2 of the *Advisory Action*. Appellant respectfully disagrees with the rejection.

As discussed further below, neither *Alt* nor *Li* teaches or suggests any implementation in which conversion and reversion are performed by first and second intermediate communication devices, as recited by claim 14. As the Examiner concedes, *Alt* proposes no such conversion or reversion. Further, the conversion that the Examiner relies upon in *Li* is expressly taught as being performed at an endpoint device, rather than being performed at an intermediate communication device. The solution proposed by *Li* is implemented by modifying the communication stack on an endpoint device. The Examiner appears to contend that one of ordinary skill in the art would have found it obvious to somehow modify the solution of *Li* to instead implement conversion and reversion at the NAT devices of *Alt*. As discussed further herein, the solution proposed by *Li* is integrated within the communication stack of an endpoint device (i.e., within the communication stack that includes a H.323 application that is executing on the endpoint device for use by an end user in performing communication). No modification to a communication stack or any other implementation solution is proposed by *Li* (or *Alt*) for performing conversion and reversion at any intermediate communication device.

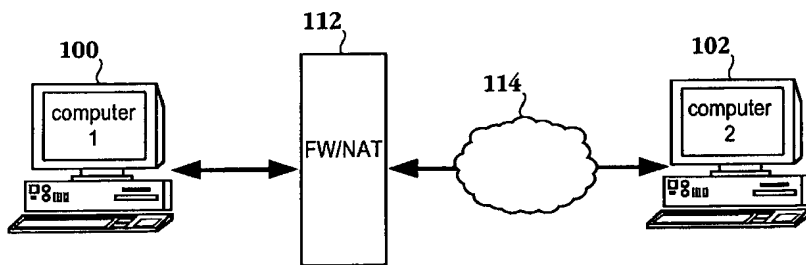
*Li* itself proposes a system that includes a NAT device, but chooses not to propose any solution for implementing conversion or reversion at such NAT device in favor of *Li*'s express teaching of instead implementing the conversion at an endpoint device. Again, *Li* implements its conversion (or "tunneling") by integrating a tunneling driver within the endpoint device's communication stack.

Thus, contrary to the Examiner's assertion, one of ordinary skill in the art would not be motivated to implement the conversion of *Li* at a NAT device of *Alt* because *Li* instead expressly teaches one of ordinary skill in the art a solution that is to be implemented at the endpoint devices (i.e., by integrating a tunneling driver in the communication stack of the endpoint device). Neither *Alt* nor *Li* proposes any solution for conversion and reversion that is taught as being implemented at an intermediate communication device, and thus one of ordinary skill in the art has no teaching whatsoever from these references regarding how such a solution might be implemented.

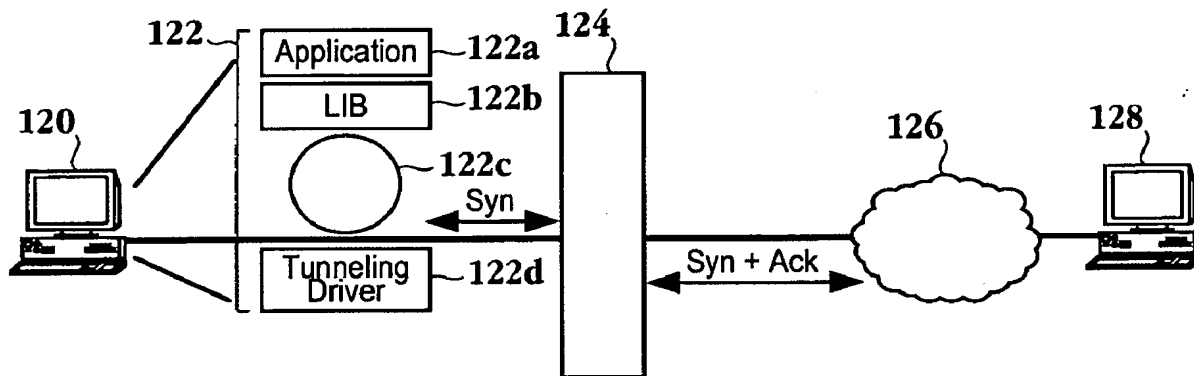
Thus, absent improper hindsight in which the disclosure of the present application is used as a blueprint or road map, one of ordinary skill in the art would simply be led to employ the tunneling of *Li* by implementing the modified communication stack at an endpoint device (as expressly taught by *Li*) within *Alt*. Accordingly, the combined disclosures of *Alt* and *Li*, when considered as a whole, fail

to teach or suggest any conversion or reversion at any intermediate communication device in the manner recited by claim 14.

As the Examiner concedes, *Alt* does not teach or suggest any such converting or reversion. Instead, the NAT devices of *Alt* are merely asserted by the Examiner as translating ports/addresses of multiport packets. *Li* likewise fails to teach or suggest any such converting or reversion by intermediate communication devices, as recited by claim 14. Instead, *Li* proposes implementing a revised communication stack at the endpoint devices (e.g., at PCs 120 and 128 of Fig. 3 of *Li*) without any first or second intermediate communication devices for converting or reversion. *Li* expressly recognizes a firewall/NAT device (112), *see* Fig. 2 of *Li* reproduced as follows:

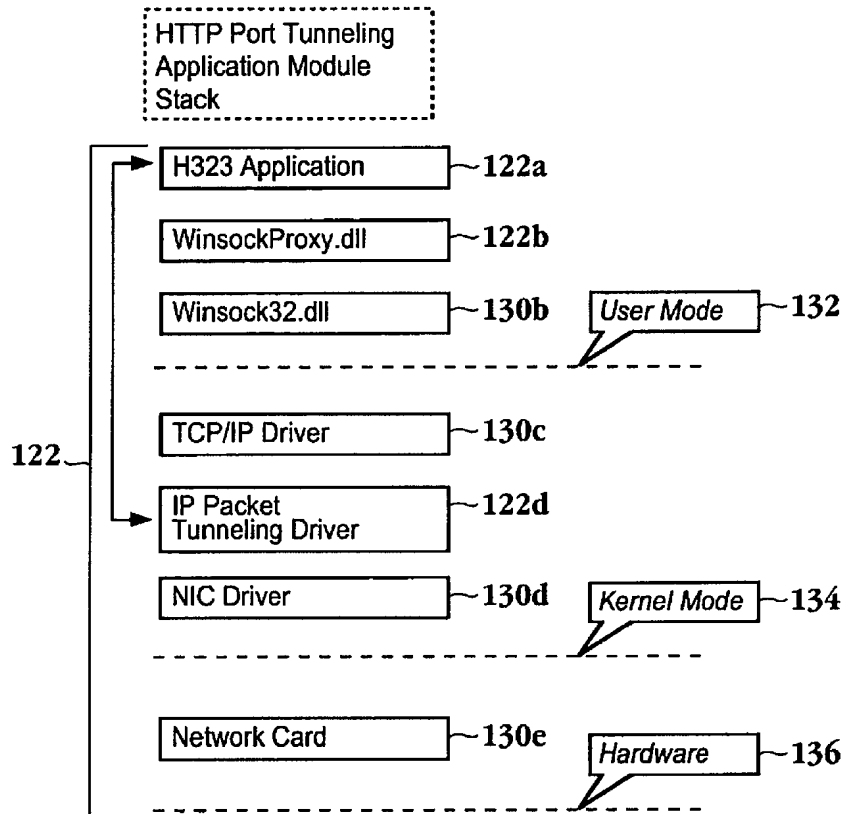


However, *Li* offers no suggestion whatsoever of implementing any converting/reversion on such NAT device 112, but instead consistently teaches implementing its tunneling via a modified communication stack on an endpoint device. As shown in the following Fig. 3 of *Li*, *Li* consistently proposes to employ a modified communication stack (122) on the endpoint device (PC 120):





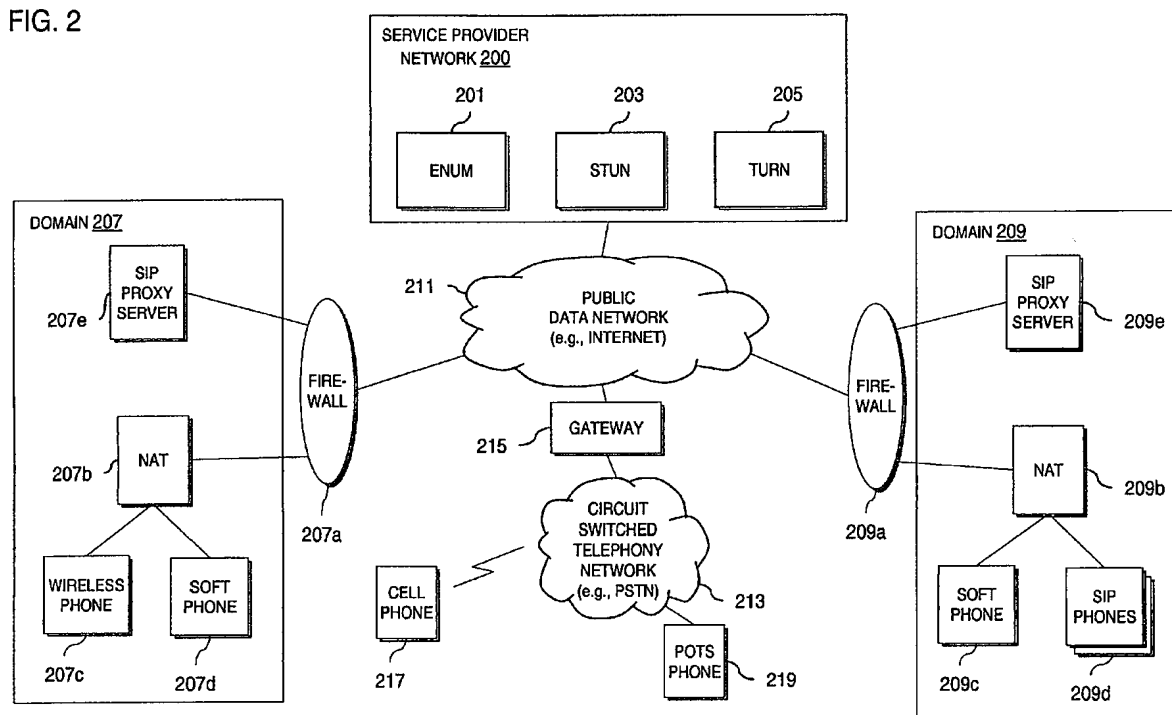
The proposed modified stack 122 is further shown in Fig. 4B of *Li*, which is reproduced as follows:



This modified stack 122 includes a modified kernel mode 134 that works with the user mode (which includes the H.323 application 122a being used by the end user) on the endpoint device (PC 120). As can be seen from the above Fig. 4B of *Li*, the HTTP port tunneling application module stack that *Li* proposes implements an IP Packet Tunneling Driver 122d in the communication stack 122 of the endpoint device 120, which further contains the H.323 application 122a that a user may be using on the endpoint device for communication. Thus, the solution proposed by *Li* expressly teaches a solution that integrates the IP Packet Tunneling Driver 122d (which performs the “conversion” asserted by the Examiner) in the endpoint device’s communication stack 122.

There is simply no suggestion whatsoever in *Li* of any implementation in which converting/reconverting is performed on an intermediate communication device, such as on a NAT device. Instead, *Li*’s solution modifies the communication stack on the endpoint device (PC 120).

Figure 2 of *Alt* shows a network, as follows:



Consistent with the express teaching of *Li*, one of ordinary skill in the art would have been motivated to implement *Li*'s modified communication stack 122 on one or more of the endpoint devices (207c, 207d, 209c, 209d) that have the H.323 application 122a running thereon, rather than somehow modify *Li*'s teaching (in a manner not taught or suggested by *Li* or *Alt*) to provide some form of converting/reconverting on the NAT devices 207b, 209b of *Alt*.

Therefore, the applied combination does not, in any way, teach or suggest the above-emphasized limitations of claim 14.

The *Advisory Action* contends that the converting of *Li* may be implemented on the NAT devices of *Alt*, and thus concludes that this modification to the combined teachings satisfies the recited converting and reconverting on intermediate communication devices, as recited by claim 14. Such assertion ignores, however, that *Li* expressly teaches a solution which integrates the driver that performs the conversion (i.e., the IP Packet Tunneling Driver 122d shown in Fig. 4B of *Li*) into the

communication stack 122 that includes the H.323 communication application being used for communication by an end user of endpoint device 120.

In apparent support of the Examiner's contention that the solution of *Li* could be implemented on a NAT device of *Alt*, the *Advisory Action* notes that *Li* asserts that its "invention can be implemented in numerous ways, including as a process, an apparatus, a system, a device, a method, a communication protocol, or a computer readable media" (paragraph 0008 of *Li*). The *Advisory Action* goes on to contend that this statement in *Li* means that the "method [of *Li*] would be implemented on whatever device would be desired to provide that functionality", and thus concludes that on this basis it would have been obvious to one of ordinary skill in the art to implement the tunneling of *Li* on the NAT devices of *Alt*. See page 2 of the *Advisory Action*.

While *Li* states that its invention can be implemented in numerous ways, including as a method, neither *Li* nor *Alt* provides any teaching or suggestion whatsoever of implementing *Li*'s tunneling on any intermediate communication devices. Instead, as discussed above, *Li* only discloses implementations in which it modifies the communication stack of an endpoint device (e.g., at PCs 120 and 128 of Fig. 3 of *Li*). One of ordinary skill in the art would not have been motivated to implement the revised communication stack of *Li* in any intermediate communication devices of *Alt*, such as *Alt*'s NAT devices. Instead, if the solution proposed in *Li* were to be implemented in *Alt*, *Li*'s express teaching would lead one of ordinary skill in the art to implement the revised communication stack of *Li* on an endpoint communication device, as discussed above.

The mere statement in *Li* that its invention may be implemented in numerous ways, including as a method, does not provide any objective reasoning for one of ordinary skill in the art to modify the express teachings of *Li* to implement its tunneling solution on an intermediate communication device instead of on the endpoint devices, and particularly not on the NAT devices which *Li* recognized (see Fig. 2 of *Li*) but expressly chose not to modify. Further, neither *Li* nor *Alt* teach or suggest any solution for converting/reconverting that is not integrated within the communication stack of an endpoint device (in the manner proposed by *Li*). Thus, the rejection of claim 14 should be overturned.

In addition, claim 14 recites "establishing a first communication connection between a first internal controller behind a firewall and a first external controller in a first communication community ... wherein a first communication request is initiated by a local communication device connected to the first internal controller", and claim 14 further recites "establishing a second communication connection between a second internal controller behind a second firewall and a second external controller in a second communication community ... wherein a second communication request is

initiated by a remote communication device connected to the second internal controller”. Claim 14 further recites that “responsive to one or more of the first and second communication request requesting communication between the local communication device and the remote communication device, establishing a third communication connection between the first and second external communication controllers; and transmitting communication data between the first and second communication communities through the third communication connection.”

As one example, the discussion of FIG. 8 of the present application (*see e.g.*, paragraphs 0045-0049) provides one exemplary scenario wherein a first communication connection is established between a first internal controller (back end 808) behind a firewall and a first external controller (front end controller 806) in a first communication community (community 82) ... wherein a first communication request is initiated by a local communication device (device 816) connected to the first internal controller. In the exemplary scenario, a second communication connection is established between a second internal controller (back end controller 811) behind a second firewall and a second external controller (front end controller 804) in a second communication community (community 83) ... wherein a second communication request is initiated by a remote communication device (device 818) connected to the second internal controller. In the exemplary scenario, a third communication connection is formed between the front end controller 806 and the front end controller 804 (e.g., via front end controller 800 in the illustrated example), and communication data is transmitted between the devices 816 and 818 in the two communities 82, 83 through the third communication connection.

Neither *Alt* nor *Li* appear to propose a scenario in which a communication request is initiated by a first communication device (e.g., device 816) for establishing a first communication between a first internal controller (back end 808) and a first external controller (front end 806), and where a second communication request is initiated by a second communication device (e.g., device 818) for establishing a second communication between a second internal controller (back end 811) and a second external controller (front end 804). Instead, it appears that all of the communication connections in *Alt* and *Li* are initiated by the request of a single calling/sending party.

Neither *Alt* nor *Li* appear to propose a scenario in which a first communication device (e.g., device 816 of FIG. 8) initiates a connection between a first internal controller (back end 808) and a first external controller (front end 806), and where a second communication device (e.g., device 818 of FIG. 8) initiates a connection between a second internal controller (back end 81) and a second external controller (front end 804). As discussed in the exemplary scenario of FIG. 8 in the present application, a first device (device 816) that desires to participate in a video conference call may initiate a

Application No. 11/403,548

Docket No.: 69936/P002US/10601229

connection between back end controller 808 and front end controller 806 in its communication community 82, and a second device (device 818) that desires to participate in the video conference call may initiate a connection between back end controller 811 and front end controller 804 in its communication community 83.

No such initiation of connections by different communication devices appears to be taught or suggested by *Alt* and *Li*. Instead, it appears that all of the communication connections in *Alt* and *Li* are initiated by the request of a single calling/sending device. For instance, the called/receiving devices appear to answer the call or otherwise have connections established that are initiated by the calling device. Thus, the rejection of claim 14 should be overturned for this further reason.

Claims 15-16, 22, and 23 each depends either directly or indirectly from independent claim 14, and thus each inherits all limitations of claim 14. Therefore, dependent claims 15-16, 22, and 23 are believed allowable over the applied combination of *Alt* and *Li* based at least on their dependency from claim 14 for the reasons presented above.

**B. Rejections Under 35 U.S.C. §103 over *Alt* in view of *Aasman* and *Li***

Claims 1-5 and 9-13, and 19-21 are rejected under 35 U.S.C. § 103(a) as being unpatentable over *Alt* in view of *Aasman* and further in view of *Li*. Appellant respectfully traverses these rejections for the reasons below.

**Independent Claim 1 and Dependent Claims 2-5 and 20-21**

Independent claim 1 recites:

A method for a multimedia communication comprising:  
receiving, at a controller that is behind a firewall and that is communicatively coupled with a plurality of endpoint communication devices, a plurality of multiport packets of data in a multiport communication protocol for communication from at least one of the plurality of endpoint communication devices;  
converting, by said controller, said plurality of multiport packets into a plurality of single-port packets in a single-port communication protocol;  
receiving at an external controller a communication request from said controller behind said firewall, wherein said external controller is not behind said firewall;  
establishing a communication channel between said controller and said external controller;  
opening a second communication channel between said external controller and at least one other controller behind another firewall, wherein said at least one other controller is configured to service a single endpoint communication device;  
transmitting multimedia communication data between said controller and said at least one other controller wherein said multimedia communication data passes through said external controller; and  
distributing said multimedia communication data to one or more of said plurality of endpoint communication devices and said single endpoint communication device. (Emphasis added).

The applied combination of *Alt*, *Aasman*, and *Li* fails to teach or suggest at least the above-emphasized limitations of claim 1. For instance, neither reference teaches or suggests converting, by a controller that is behind a firewall and that is communicatively coupled with a plurality of endpoint communication devices, a plurality of multiport packets into a plurality of single-port packets in a single-port communication protocol.

As discussed in greater detail above with claim 14, *Li* does not teach or suggest any such controller that is communicatively coupled with a plurality of endpoint communication devices which performs any such converting, but instead *Li* expressly teaches a solution in which a modified communication stack 122 is implemented on an endpoint communication device 120, where the

modified communication stack 122 integrates therein a driver 122d for tunneling communication through a firewall.

The Examiner does not rely upon *Alt* or *Aasman* for teaching or suggesting such conversion by a controller, as those references also fail to provide any teaching or suggestion of that limitation. As such, the applied combination fails to teach or suggest at least the above-identified limitation.

Further, as discussed in greater detail above with claim 14, one of ordinary skill in the art would not have been motivated to modify the teaching of *Li* to employ its conversion in a controller, such as that recited by claim 1, but would have instead been motivated based on the express teaching of *Li* to implement the conversion driver (122d) in an endpoint device (such as the endpoint devices in *Alt*). This is particularly true since there is simply no teaching whatsoever in any of the references regarding how one might modify a controller (such as the NAT device of *Alt*) to achieve a conversion solution, nor has any objective reasoning been identified regarding why one of ordinary skill in the art would have undertaken such a modification instead of merely implementing the modified communication stack within an endpoint device as taught by *Li*.

Thus, at least for the above reasons the rejection of independent claim 1 should be overturned.

Claims 2-5 and 20-21 each depends either directly or indirectly from independent claim 1, and thus each inherits all limitations of claim 1. Therefore, dependent claims 2-5 and 20-21 are believed allowable over the applied combination of *Alt*, *Aasman*, and *Li* based at least on their dependency from claim 1 for the reasons presented above.

**Independent Claim 9 and Dependent Claims 10-13 and 19**

Independent claim 9, as amended herein, recites:

A communication community comprising:  
one or more shared controllers connected to one or more endpoint communication devices, wherein said one or more shared controllers is behind a firewall, and wherein said one or more shared controllers is operable to convert a plurality of multiport packets received from said one or more endpoint communication devices into a plurality of single-port packets in a single-port communication protocol;  
at least one individual controller connected to a single endpoint communication device, wherein said at least one individual controller is behind another firewall, and wherein said at least one individual controller is operable to reconvert said plurality of single-port packets into said multiport communication protocol, resulting in reconverted plurality of multiport packets, and transmit to said single endpoint communication device said reconverted plurality of multiport packets using two or more ports associated with said multiport communication protocol; and  
an external controller that comprises a device, said external controller in connection to said one or more shared controllers and said at least one individual controller, wherein said external controller is not behind said firewall or said another firewall, and wherein said external controller facilitates communication between ones of said one or more endpoint communication devices and said single endpoint communication device. (Emphasis added).

The applied combination of *Alt*, *Aasman*, and *Li* fails to teach or suggest at least the above-emphasized limitations of claim 9. For instance, neither reference teaches or suggests converting, by shared controller(s) that are behind a firewall and that are connected to one or more endpoint communication devices, a plurality of multiport packets received from said one or more endpoint communication devices into a plurality of single-port packets in a single-port communication protocol.

Further, neither reference teaches or suggests reconverting, by at least one individual controller that is behind another firewall and that is connected to a single endpoint communication device, the plurality of single-port packets into the multiport communication protocol, resulting in reconverted plurality of multiport packets, and transmitting to a single endpoint communication device the reconverted plurality of multiport packets using two or more ports associated with the multiport communication protocol.

As discussed in greater detail above with claim 14, *Li* does not teach or suggest any such shared or individual controllers that are communicatively coupled with endpoint communication devices for performing any such converting or reconverting, as recited by claim 9, but instead *Li*



Application No. 11/403,548

Docket No.: 69936/P002US/10601229

expressly teaches a solution in which a modified stack 122 is implemented on an endpoint communication device 120, where the modified communication stack 122 integrates therein a driver 122d for tunneling communication through a firewall.

The Examiner does not rely upon *Alt* or *Aasman* for teaching or suggesting such converting or reconverting by controllers (as recited by claim 9), as those references also fail to provide any teaching or suggestion of those limitations. As such, the applied combination fails to teach or suggest at least the above-identified limitations.

Further, as discussed in greater detail above with claim 14, one of ordinary skill in the art would not have been motivated to modify the teaching of *Li* to employ its conversion in a controller, such as that recited by claim 9, but would have instead been motivated based on the express teaching of *Li* to implement the conversion driver (122d) in an endpoint device (such as the endpoint devices in *Alt*). This is particularly true since there is simply no teaching whatsoever in any of the references regarding how one might modify a controller (such as the NAT device of *Alt*) to achieve a conversion and reversion solution, nor has any objective reasoning been identified regarding why one of ordinary skill in the art would have undertaken such a modification instead of merely implementing the modified communication stack within an endpoint device as taught by *Li*.

Thus, at least for this reason the rejection of independent claim 9 should be overturned.

Claims 10-13 and 19 each depends either directly or indirectly from independent claim 9, and thus each inherits all limitations of claim 9. Therefore, dependent claims 10-13 and 19 are believed allowable over the applied combination of *Alt*, *Aasman*, and *Li* based at least on their dependency from claim 9 for the reasons presented above.

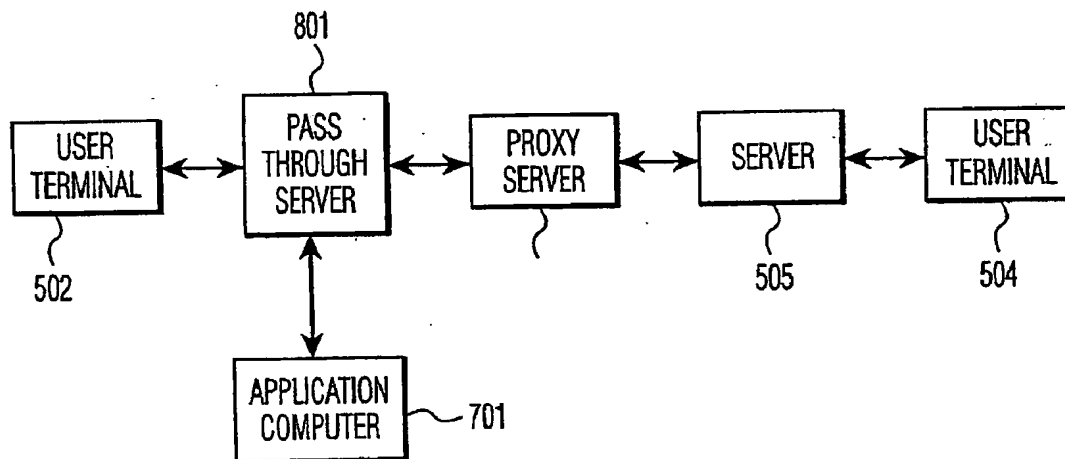
**C. Rejections Under 35 U.S.C. §103 over *Alt* in view of *Strathmeyer* and *Li***

Claims 17 and 18 are rejected under 35 U.S.C. § 103(a) as being unpatentable over *Alt* in view of *Li* and further in view of *Strathmeyer*. Each of dependent claims 17 and 18 depends either directly or indirectly from independent claim 14, and thus each inherits all limitations of claim 14. It is respectfully submitted that dependent claims 17 and 18 are thus allowable at least because of their dependency from independent claim 14 for the reasons discussed above.

In addition, claim 17 further recites:

The method of claim 14 wherein said establishing a third communication connection comprises:  
issuing a third communication request to a central communication controller;  
establishing a first central communication channel between said first external controller and said central communication controller;  
issuing a fourth communication request from said central communication controller to said second external controller; and  
establishing a second central communication channel between said central communication controller and said second external controller.

The Examiner relies upon *Strathmeyer* as teaching or suggesting the operations recited in claim 17. The Examiner appears to contend that Fig. 7 of *Strathmeyer* provides one example of disclosing the above operations. Fig. 7 of *Strathmeyer* is reproduced as follows:



The Examiner contends “the proxy server may correspond to the first external controller and the server 505 may correspond to the central controller”. Page 12 of the Final Office Action. Without conceding that this characterization by the Examiner is correct, Appellant notes that it falls short of

teaching or suggesting all limitations of claim 15. For instance, even under the Examiner's characterization that the Proxy server of *Strathmeyer* is a first external controller and the server 505 of *Strathmeyer* is a central controller, Fig. 7 merely shows a connection between the first external controller (proxy server) and the central controller (server 505), and fails to teach or suggest "issuing a fourth communication request from said central communication controller to said second external controller; and establishing a second central communication channel between said central communication controller and said second external controller" (emphasis added), as recited by claim 15. For instance, no such second external controller with which a second communication channel is established with the central communication controller (server 505) is taught or suggested in Fig. 7 of *Strathmeyer*. Rather, the server 505 is shown in Fig. 7 (which is relied upon by the Examiner) as coupled to the proxy server (the asserted first external controller) and a user terminal 504.

Thus, the rejection of claim 17 should be overturned for this further reason. Claim 18 depends from claim 17 and thus inherits all limitations of claim 17, and therefore the rejection of claim 18 should likewise be overturned for this further reason.

#### **D. Rejections Under 35 U.S.C. §103 over *Alt* in view of *Aasman*, *Li*, and *Strathmeyer***

Claims 6-8 are rejected under 35 U.S.C. § 103(a) as being unpatentable over *Alt* in view of *Aasman* and *Li* and further in view of *Strathmeyer*. Each of dependent claims 6-8 depends either directly or indirectly from independent claim 1, and thus each inherits all limitations of claim 1. It is respectfully submitted that dependent claims 6-8 are thus allowable at least because of their dependency from independent claim 1 for the reasons discussed above.

In addition, the rejection of claims 6-7 appear inconsistent, at best. In rejecting claim 6, the Examiner concedes (on pages 24-25 of the Final Office Action) that the combination of *Alt*, *Li*, and *Aasman* fails to disclose the recited request from the external controller to a central controller, nor the recited receiving of multimedia communication data at the central controller. Instead, the Examiner relies upon *Strathmeyer* as disclosing the recited external controller, in a manner similar to that discussed above with claim 15.

However, in rejecting claim 7 (which depends from claim 6), the Examiner appears to contend that *Alt* discloses the determining a peripheral controller connected to said external endpoint device; opening another external channel between said central controller and said peripheral controller; and forwarding said multimedia communication data to the peripheral controller from said central

Application No. 11/403,548

Docket No.: 69936/P002US/10601229

controller. Appellant fails to understand how *Alt* can possibly teach or suggest the limitations of claim 7 when the Examiner appears to concede in the treatment of claim 6 that *Alt* fails to teach or suggest the central controller that is introduced in claim 6 (which is the central controller referenced as “said central controller” in claim 7, which depends from claim 6). The Examiner’s explanation regarding claim 7 merely contends that “entities in the service provider network may be construed as the central controller” (*see* page 26 of the Final Office Action) without any further specification as to which entities in the service provider network of *Alt* satisfy the limitations of claims 6 and 7 concerning the operations performed with the central controller.

As a result of the inconsistency in the assertions in the Final Office Action, it is unclear to Appellant exactly how the Examiner is contending that the various elements/components of the applied references are mapped to the recited limitations of the claims. The Examiner appears to, at best, assert that some entity in the service provider network of *Alt* may be construed as the central controller (*see* page 26 of the Final Office Action), without specifically designating which such entity the Examiner contends as satisfying the recited limitations, thereby leaving it to Appellant (and the Board) to guess at how the various components of the applied combination of references are being mapped to the claim limitations in the Examiner’s rejection.

Thus, the rejection of claims 6-8 should be overturned for this further reasoning and lack of clarity in the Examiner’s rejection.

Also, as similarly discussed above with claim 17, *Strathmeyer* fails to teach or suggest that its server 505 (which the Examiner appears to contend is the recited central controller in the treatment of claims 6 and 17) has a communication channel with an external controller AND another controller (such as the recited peripheral controller of claim 7. Thus, the rejection of claim 7 should be overturned for this further reason.

Application No. 11/403,548

Docket No.: 69936/P002US/10601229

**Conclusion**

In view of the above, Appellant requests that the board overturn the outstanding rejections of claims 1-23. Attached hereto are a Claims Appendix, Evidence Appendix, and Related Proceedings Appendix. As noted in the attached Evidence Appendix, no evidence pursuant to §§ 1.130, 1.131, or 1.132 or entered by or relied upon by the examiner is being submitted. Also, as noted in Section II of this appeal brief, Appellant is aware of no related proceedings, and thus no decisions in any such related proceedings are provided.

Dated: May 26, 2010

Respectfully submitted,

By 

Jody C. Bishop

Registration No.: 44,034

FULBRIGHT & JAWORSKI L.L.P.

2200 Ross Avenue, Suite 2800

Dallas, Texas 75201-2784

Tel: (214) 855-8007; Fax: (214) 855-8200

Attorneys for Applicant

## **VIII. Claims Appendix**

### **Claims Involved in the Appeal of Application Serial No. 11/403,548**

1. A method for a multimedia communication comprising:

receiving, at a controller that is behind a firewall and that is communicatively coupled with a plurality of endpoint communication devices, a plurality of multiport packets of data in a multiport communication protocol for communication from at least one of the plurality of endpoint communication devices;

converting, by said controller, said plurality of multiport packets into a plurality of single-port packets in a single-port communication protocol;

receiving at an external controller a communication request from said controller behind said firewall, wherein said external controller is not behind said firewall;

establishing a communication channel between said controller and said external controller;

opening a second communication channel between said external controller and at least one other controller behind another firewall, wherein said at least one other controller is configured to service a single endpoint communication device;

transmitting multimedia communication data between said controller and said at least one other controller wherein said multimedia communication data passes through said external controller; and

distributing said multimedia communication data to one or more of said plurality of endpoint communication devices and said single endpoint communication device.

2. The method of claim 1 further comprising:

verifying said communication request at said external controller.

3. The method of claim 1 further comprising:

transmitting a security key from said controller to said external controller for authorization of said communication request.

4. The method of claim 1 further comprising:

sending an external request from said external controller to an additional external controller responsive to said communication request requesting to communicate with an additional endpoint communication device connected to said additional external controller.

5. The method of claim 4 further comprising:  
establishing an external channel between said external controller and said additional external controller; and

forwarding said multimedia communication data to said additional external controller from said external controller; and

distributing said multimedia communication data to said additional endpoint communication device.

6. The method of claim 1 further comprising:  
issuing a central request from said external controller to a central controller responsive to said communication request requesting to communicate with an external endpoint device not connected to one or more of said controller and said at least one other controller; and

receiving said multimedia communication data at said central controller.

7. The method of claim 6 further comprising:  
determining a peripheral controller connected to said external endpoint device;  
opening another external channel between said central controller and said peripheral controller;

forwarding said multimedia communication data to said peripheral controller from said central controller; and

distributing said multimedia communication data to said external endpoint device.

8. The method of claim 6 further comprising:  
distributing said multimedia communication data to said external endpoint device when said external endpoint device is connected to said central controller.

9. A communication community comprising:

one or more shared controllers connected to one or more endpoint communication devices, wherein said one or more shared controllers is behind a firewall, and wherein said one or more shared controllers is operable to convert a plurality of multiport packets received from said one or more endpoint communication devices into a plurality of single-port packets in a single-port communication protocol;

at least one individual controller connected to a single endpoint communication device, wherein said at least one individual controller is behind another firewall, and wherein said at least one individual controller is operable to reconvert said plurality of single-port packets into said multiport communication protocol, resulting in reconverted plurality of multiport packets, and transmit to said single endpoint communication device said reconverted plurality of multiport packets using two or more ports associated with said multiport communication protocol; and

an external controller that comprises a device, said external controller in connection to said one or more shared controllers and said at least one individual controller, wherein said external controller is not behind said firewall or said another firewall, and wherein said external controller facilitates communication between ones of said one or more endpoint communication devices and said single endpoint communication device.

10. The communication community of claim 9 further comprising:

a verification utility within said external controller for verifying one or more communication requests from one or more of said one or more shared controllers and said individual controller.

11. The communication community of claim 9 further comprising:

a security key repository within each of said one or more shared controllers and said individual controller, wherein said one or more shared controllers and said individual controller transmit a security key for verification by said external controller for each communication request issued to said external controller.

12. The communication community of claim 9 further comprising:

an external communication interface within said external controller for communicating with a second communication community.



Application No. 11/403,548

Docket No.: 69936/P002US/10601229

13. The communication community of claim 12 wherein said external controller communicates with a central communication controller to establish a communication channel with said second communication community.

14. A method for communicating comprising:

establishing a first communication connection between a first internal controller behind a firewall and a first external controller in a first communication community, said first external controller not behind said firewall, wherein a first communication request is initiated by a local communication device connected to the first internal controller;

establishing a second communication connection between a second internal controller behind a second firewall and a second external controller in a second communication community, said second external controller not behind said second firewall, wherein a second communication request is initiated by a remote communication device connected to the second internal controller;

responsive to one or more of the first and second communication request requesting communication between the local communication device and the remote communication device, establishing a third communication connection between the first and second external communication controllers; and

transmitting communication data between the first and second communication communities through the third communication connection, wherein said transmitting comprises:

receiving, at a first intermediate communication device that is behind said firewall a plurality of multiport packets of data in a multiport communication protocol for communication from said local communication device in said first communication community,

converting, by said first intermediate communication device, said plurality of multiport packets into a plurality of single-port packets in a single-port communication protocol,

transmitting, through the third communication connection, said plurality of single-port packets to a second intermediate communication device that is behind said second firewall,

receiving said plurality of single-port packets at said second intermediate communication device,

reconverting, by said second intermediate communication device, said received plurality of single-port packets into said multiport communication protocol, resulting in reconverted plurality of multiport packets, and

delivering, from said second intermediate communication device to said remote communication device in said second communication community, said reconverted plurality of multiport packets using two or more ports associated with said multiport communication protocol.

15. The method of claim 14 further comprising:

verifying at said first external controller said first communication request prior to said establishing said first communication connection; and

verifying at said second external controller said second communication request prior to said establishing said second communication connection.

16. The method of claim 15 further comprising:

issuing a third communication request between said first and second external controllers; and  
verifying said third communication request prior to said establishing said third communication connection.

17. The method of claim 14 wherein said establishing a third communication connection comprises:

issuing a third communication request to a central communication controller;

establishing a first central communication channel between said first external controller and said central communication controller;

issuing a fourth communication request from said central communication controller to said second external controller; and

establishing a second central communication channel between said central communication controller and said second external controller.

18. The method of claim 17 further comprising:

verifying said third communication request at said central communication controller prior to said establishing said first central communication channel;

verifying said fourth communication request prior to said establishing said second central communication channel.

19. The communication community of claim 9 wherein said one or more shared controllers, and said at least one individual controller each comprise a device.

20. The method of claim 1 wherein said transmitting said multimedia communication data between said controller and said at least one other controller comprises:

transmitting from said controller said plurality of single-port packets over a commonly-open port to said at least one other controller, said plurality of single-port packets traversing one or more firewalls using said commonly-open port.

21. The method of claim 20 further comprising:

receiving said plurality of single-port packets at said at least one other controller;

reconverting, by said at least one other controller, said received plurality of single-port packets into said multiport communication protocol, resulting in reconverted plurality of multiport packets; and

delivering, from said at least one other controller to said single endpoint communication device, said reconverted plurality of multiport packets using two or more ports associated with said multiport communication protocol.

22. The method of claim 14 wherein said first internal controller comprises said first intermediate communication device; and wherein said second internal controller comprises said second intermediate communication device.

23. The method of claim 14 wherein said transmitting, through the third communication connection, said plurality of single-port packets to a second intermediate communication device that is behind said second firewall comprises:

transmitting said plurality of single-port packets over a commonly-open port.

Application No. 11/403,548

Docket No.: 69936/P002US/10601229

### **IX. Evidence appendix**

No evidence pursuant to §§ 1.130, 1.131, or 1.132 or entered by or relied upon by the examiner is being submitted.

Application No. 11/403,548

Docket No.: 69936/P002US/10601229

### **X. Related Proceedings Appendix**

Appellant is aware of no other appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

# **EXHIBIT 11**

---

**From:** Ferenc, Christopher B. <christopher.ferenc@kattenlaw.com>  
**Sent:** Thursday, June 27, 2019 3:41 PM  
**To:** Ganguly, Tuhin; Datta, Suparna  
**Cc:** Honasoge, Yashas K.; Ross, Terence P.; Wooden, Sean S.; Noona, Stephen E.; Polycom\_Pepper; gbryant@wilsav.com; johana@wilsav.com; Datta, Suparna  
**Subject:** [EXTERNAL] RE: Re: directPacket v. Polycom | Deficiencies in directPacket's Infringement Contentions, Conception & RTP Disclosures, and Claim Construction Disclosures

Tuhin,

You seem to misunderstand what I am telling you. Under the Court's Rule 16(b) Scheduling Order (Dkt. No. 32), Polycom was required to disclose to us the construction it proposed for each term at issue. Polycom did this on June 13, 2019 and then revised certain constructions on June 19, 2019 as a result of the parties' meet and confer on June 18, 2019. Polycom is now stuck with the proposed construction it disclosed on June 19, 2019. In Polycom's claim construction briefing, it can only argue for the proposed construction disclosed on June 19, 2019. Polycom cannot now argue for a different proposed construction as you seek to do. directPacket relied on Polycom's proposed claim construction disclosed on June 19, 2019 in preparing its opening claim construction brief due tomorrow. directPacket has devoted significant time and resources to drafting its opening brief to meet tomorrow's deadline, including working with its expert to consider the proposed constructions offered by the parties. That was the reason that the Court ordered disclosure of proposed constructions by the parties. Any deviation from what Polycom proposed on June 19, 2019 would prejudice directPacket. And, if Polycom argues for any claim construction other than exactly what it disclosed on June 19, 2019, it will be in violation of a Court Order. We will move to strike your claim construction brief and for sanctions. Polycom must stop acting as if it is free to disregard Court orders. Please abide by the Court's Rule 16(b) Scheduling Order or face the consequences.

Regards,

Chris

**Christopher B. Ferenc**

Associate

**Katten Muchin Rosenman LLP**

2900 K Street NW, North Tower - Suite 200 / Washington, DC 20007-5118

p / +1.202.625.3647 f / +1.202.339.6044

[christopher.ferenc@kattenlaw.com](mailto:christopher.ferenc@kattenlaw.com) / [www.kattenlaw.com](http://www.kattenlaw.com)

---

**From:** Ganguly, Tuhin <gangulyt@pepperlaw.com>

**Sent:** Thursday, June 27, 2019 12:16 AM

**To:** Ferenc, Christopher B. <christopher.ferenc@kattenlaw.com>; Datta, Suparna <dattas@pepperlaw.com>

**Cc:** Honasoge, Yashas K. <yashas.honasoge@kattenlaw.com>; Ross, Terence P. <terence.ross@kattenlaw.com>;

Wooden, Sean S. <sean.wooden@kattenlaw.com>; Noona, Stephen E. <senoona@kaufcan.com>; Polycom\_Pepper

<Polycom\_Pepper@pepperlaw.com>; gbryant@wilsav.com; johana@wilsav.com; Datta, Suparna <no-reply@sharepointonline.com>

**Subject:** RE: Re: directPacket v. Polycom | Deficiencies in directPacket's Infringement Contentions, Conception & RTP Disclosures, and Claim Construction Disclosures

Chris,



Setting your aspersions aside, our hope was to narrow the issues and potentially reach agreement, which we believe the Court would appreciate. Indeed, this is the purpose of the parties' meeting and conferring during the claim construction process.

In particular, there were three issues raised by our original construction: (i) whether each of the protocols must be different, (ii) whether the protocols include a signaling protocol, and (iii) the meaning of "protocol." We agreed to directPacket's proposed construction of protocol in order to move the parties' constructions closer. In coming to an agreement on that issue, we now believe the signaling protocol issue to be moot with respect to this claim term. Accordingly, there is now only a single issue to be decided by the Court – whether each of the protocols needs to be different, which we have always contended they do. If you contend that the three protocols are not required to be different, please let us know. Otherwise, please let us know if there is any reason you cannot agree to our proposed construction. By withdrawing both issues (ii) and (iii), we are decreasing the issues that must be decided as part of the Markman process, so your claim that we are expanding issues to be briefed is misplaced.

Regards,  
Tuhin

---

**From:** Ferenc, Christopher B. [<mailto:christopher.ferenc@kattenlaw.com>]  
**Sent:** Wednesday, June 26, 2019 6:18 PM  
**To:** Datta, Suparna  
**Cc:** Honasoge, Yashas K.; Ross, Terence P.; Wooden, Sean S.; Noona, Stephen E.; Ganguly, Tuhin; Polycom\_Pepper; [gbryant@wilsav.com](mailto:gbryant@wilsav.com); [johana@wilsav.com](mailto:johana@wilsav.com); Datta, Suparna  
**Subject:** [EXTERNAL] RE: Re: directPacket v. Polycom | Deficiencies in directPacket's Infringement Contentions, Conception & RTP Disclosures, and Claim Construction Disclosures

Suparna,

Per the Court's order (Dkt. No. 104), the parties exchanged their lists of terms to be construed on June 6, 2019, agreed to exchange proposed constructions for those terms on June 13, 2019, and agreed to meet and confer on June 18, 2019 to resolve any disputes between the parties.

During the parties' June 18, 2019 meet and confer, it became clear that you lacked any authority to negotiate the list of terms to be construed. Ultimately, on June 19, 2019, Polycom agreed to the fair and reasonable proposal previously offered by directPacket prior to the meet and confer on June 18, 2019. The parties then finalized both the terms to be construed and each parties' proposed constructions thereof. Since that time, directPacket has been preparing its opening *Markman* brief based on these finalized terms and the constructions proposed by each party.

Now, just two days before opening briefs are due, Polycom is seeking to change its proposed constructions. Such a change is well past the June 13, 2019 deadline and violates the Court's order regarding claim construction. Moreover, it would significantly prejudice directPacket, which has been preparing its opening brief in the good-faith reliance on the parties' June 19, 2019 agreement.

Polycom attempts to excuse the material changes it now proposes to its June 13, 2019 proposed constructions under the pretext that it will "narrow[] issues to be briefed." We disagree. Polycom's proposed change will not narrow the issues to be briefed. In fact, it will expand them. Moreover, it will be impossible for directPacket to now change its opening brief by the deadline. Polycom's proposed change is particularly troubling given its insistence that the parties move forward with the Court's *Markman* schedule, without modification. Accordingly, directPacket does not consent to Polycom's belated proposal to materially change its June 13, 2019 proposed constructions and will brief the following proposed construction offered by Polycom:

| Term | Polycom's Proposed Construction |
|------|---------------------------------|
|------|---------------------------------|

“first/second/[interim/intermediate] protocol”

each of the first, second and [interim / intermediate] protocols includes a signaling protocol, whereby no two signaling protocols are the same, and whereby a protocol is a set of conventions governing the format of messages exchanged between two communication devices

Regards,

Chris

**Christopher B. Ferenc**

Associate

**Katten Muchin Rosenman LLP**

2900 K Street NW, North Tower - Suite 200 / Washington, DC 20007-5118

p / +1.202.625.3647 f / +1.202.339.6044

[christopher.ferenc@kattenlaw.com](mailto:christopher.ferenc@kattenlaw.com) / [www.kattenlaw.com](http://www.kattenlaw.com)

**From:** Datta, Suparna <[dattas@pepperlaw.com](mailto:dattas@pepperlaw.com)>

**Sent:** Wednesday, June 26, 2019 4:36 AM

**To:** Ferenc, Christopher B. <[christopher.ferenc@kattenlaw.com](mailto:christopher.ferenc@kattenlaw.com)>

**Cc:** Honasoge, Yashas K. <[yashas.honasoge@kattenlaw.com](mailto:yashas.honasoge@kattenlaw.com)>; Ross, Terence P. <[terence.ross@kattenlaw.com](mailto:terence.ross@kattenlaw.com)>; Wooden, Sean S. <[sean.wooden@kattenlaw.com](mailto:sean.wooden@kattenlaw.com)>; Noona, Stephen E. <[senoona@kaufcan.com](mailto:senoona@kaufcan.com)>; Ganguly, Tuhin <[gangulyt@pepperlaw.com](mailto:gangulyt@pepperlaw.com)>; Polycom\_Pepper <[Polycom\\_Pepper@pepperlaw.com](mailto:Polycom_Pepper@pepperlaw.com)>; [gbryant@wilsav.com](mailto:gbryant@wilsav.com); [johana@wilsav.com](mailto:johana@wilsav.com); Datta, Suparna <[no-reply@sharepointonline.com](mailto:no-reply@sharepointonline.com)>

**Subject:** Re: Re: directPacket v. Polycom | Deficiencies in directPacket's Infringement Contentions, Conception & RTP Disclosures, and Claim Construction Disclosures

Counsel,

In the interest of further narrowing the issues to be briefed for claim construction, Polycom will modify its construction for Term 1 “**first / second / [interim/intermediate] protocol**” (in the ‘588 Patent, claims 1, 3, 4, 6, 7, 8, 9, 11, 13, 14, 16, 17, 18, 20, 21, 23) to incorporate directPacket’s construction of protocol, to which we previously agreed, and streamline the remaining language regarding “first/second/[interim/intermediate].” To that end, our construction of this term is as follows:

- each of the first, second and [interim / intermediate] protocols is different.
- protocol is a set of conventions governing the format of messages exchanged between two communication devices.

Regards,

Suparna

**Suparna Datta, J.D., Ph.D.**

Associate

**Pepper Hamilton LLP**  
*Attorneys at Law*

19th Floor, High Street Tower | 125 High Street

Boston, Massachusetts 02110-2736

p: 617.204.5110 | f: 800.801.3934 | c: 617.506.9693

[email](#) | [map](#) | [website](#)



# **APPENDIX A**

## TABLE OF CONTENTS

|      |  |    |
|------|--|----|
| I.   | Legal Standards.....   | 1  |
| II.  | Background of the Technology.....  | 2  |
| III. | Level of Ordinary Skill in the Art.....  | 2  |
| IV.  | Claim Terms with Agreed Upon Constructions.....  | 2  |
| A.   | U.S. Patent No. 7,773,588.....   | 2  |
| 1.   | protocol (claims 1, 3, 4, 6, 7, 8, 9, 11, 13, 14, 16, 17, 18, 20, 21, 23).....   | 2  |
| V.   | Claim Terms with Disputed Constructions.....   | 3  |
| A.   | U.S. Patent No. 7,773,588.....   | 3  |
| 1.   | first / second / [interim / intermediate] protocol (claims 1, 3, 4, 6, 7, 8, 9, 11, 13, 14, 16, 17, 18, 20, 21, 23).....   | 3  |
| 2.   | converting said first protocol into an intermediate protocol (claims 1, 11, 18) / convert said first protocol into an interim protocol using said first protocol conversion table (claim 7).....   | 6  |
| 3.   | translating said intermediate protocol into a second protocol (claims 1, 11, 18) .....   | 10 |
| B.   | U.S. Patent No. 7,710,978.....   | 12 |
| 1.   | commonly-open ('978 Patent: claims 1, 10, 11, 12, 14, 21, 22; '828 Patent: claims 9, 23) .....   | 12 |
| 2.   | first /second [intermediate communication/network] device (claims 1, 14 of '978 Patent) first / second [intermediate communication / network] device (claims 1, 14 of '978 Patent).....  | 16 |
| 3.   | multiport communication protocol ('978 Patent: 1, 6, 15; '828 Patent: 1, 10, 11, 17) .....   | 17 |
| 4.   | converting ... said plurality of multiport packets into a plurality of single-port packets in a single-port communication protocol ('978 Patent: 1; '828 Patent: 1, 17); convert said plurality of multiport packets into a plurality of single-port packets in a single-port communication protocol ('978 Patent: 14); convert a plurality of |    |

|     |  |    |
|-----|--|----|
|     | multiport packets ... into a plurality of single-port packets in a single-port communication protocol ('828 Patent: 11).....   | 19 |
| 5.  | reconverting ... said received plurality of single-port packets into said multiport communication protocol ('978 Patent, claim 1; '828 Patent, claims 10, 17); reconverting said converted plurality of single-port packets into multiport communication protocol ('978 Patent, claim 14); reconvert said plurality of single-port packets into said multiport communication protocol ('828 Patent, claim 11)..... | 21 |
| C.  | U.S. Patent No. 8,560,828.....   | 22 |
| 1.  | external controller (claims 1, 2, 3, 4, 5, 11, 12, 13, 14, 15, 17 ,18, 19) .....   | 22 |
| 2.  | single endpoint communication device (claims 1, 10, 11).....   | 24 |
| VI. | Conclusion .....   | 25 |

# **APPENDIX B**

**LIST OF EXHIBITS**

| <b>Exhibit</b> | <b>Description</b>  |
|----------------|---|
| 1              | Declaration of Dr. Tal Lavian   |
| 1A             | Curriculum Vitae of Dr. Tal Lavian  |
| 2              | U.S. Patent No. 7,710,978   |
| 3              | U.S. Patent No. 7,773,588   |
| 4              | U.S. Patent No. 8,560,828   |
| 5              | Excerpt of File History of U.S. Patent No. 7,710,978 – April 13, 2009 Applicant Initiated Interview Request |
| 6              | Excerpt of File History of U.S. Patent No. 7,710,978 – Aug. 28, 2009 Amendment & Response                   |
| 7              | Excerpt of File History of U.S. Patent No. 7,773,588 – Aug. 19, 2008 Amendment & Response                   |
| 8              | Excerpt of File History of U.S. Patent No. 7,773,588 – Jan 21, 2009 Amendment & Response                    |
| 9              | Excerpt of File History of U.S. Patent No. 7,773,588 – Sept. 18, 2009 Amendment & Response                  |
| 10             | Excerpt of File History of U.S. Patent No. 8,560,828 – May 26, 2010 Appeal Brief                            |
| 11             | Email exchange between counsel for the Parties dated June 26-27, 2019                                       |

# APPENDIX C



# **TABLE OF AUTHORITIES**

|  | <b>Page(s)</b> |
|--|----------------|
| <b>CASES</b>   |                |
| <i>Ad-In-The-Hole, International v. Hageman</i> , 1997 U.S. App. LEXIS 6213 (Fed. Cir 1997) .....        | 29, 30         |
| <i>Aventis Pharms. Inc. v. Amino Chems. Ltd.</i> , 715 F.3d 1363 (Fed. Cir. 2013).....                   | 2              |
| <i>Ekchian v. Home Depot, Inc.</i> , 104 F.3d 1299 (Fed. Cir. 1997) .....                                | 10             |
| <i>Eon Corp. IP Holdings LLC v. Silver Spring Networks, Inc.</i> , 815 F.3d 1314 (Fed. Cir. 2016) .....  | 20, 28         |
| <i>Ethicon Endo-Surgery, Inc. v. United States Surgical Corp.</i> , 93 F.3d 1572 (Fed. Cir. 1996) .....  | 5              |
| <i>Exxon Chemical Patents, Inc. v. Lubrizol Corp.</i> , 64 F.3d 1553 (Fed. Cir. 1995).....               | 5              |
| <i>Gentry Gallery, Inc. v. Berkline Corp.</i> , 134 F.3d 1473 (Fed. Cir. 1998).....                      | 21, 28         |
| <i>Luminara Worldwide, LLC v. Liown Elecs. Co.</i> , 814 F.3d 1343 (Fed. Cir. 2016).....                 | 7              |
| <i>Markman v. Westview Instruments, Inc.</i> , 517 U.S. 370 (1996) .....                                 | 1              |
| <i>Nautilus, Inc. v. Biosig Instruments, Inc.</i> 572 U.S. 898 (2014) .....                              | 15             |
| <i>Nystrom v. TREX Co.</i> , 424 F.3d 1136 (Fed. Cir. 2005) .....  | 1              |
| <i>O2 Micro Int’l Ltd. v. Beyond Innovation Tech. Co.</i> , 521 F.3d 1351 (Fed. Cir. 2008) .....         | 27, 29         |
| <i>On-Line Techs., Inc. v. Bodenseewerk Perkin-Elmer GmbH</i> , 386 F.3d 1133 (Fed. Cir. 2004) .....     | 15             |
| <i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005) (en banc) .....                            | 1, 2           |
| <i>Ruckus Wireless, Inc. v. Innovative Wireless Solutions, LLC</i> , 824 F.3d 999 (Fed. Cir. 2016) ..... | 21, 28         |
| <i>Tate Access Floors v. Interface Architectural Res.</i> , 279 F.3d 1357 (Fed. Cir. 2002).....          | 30             |
| <i>Varco, L.P. v. Pason Sys. USA Corp.</i> , 436 F.3d 1368 (Fed. Cir. 2006) .....                        | 12             |
| <i>Vitronics Corp. v. Conceptronic</i> , 90 F.3d 1576 (Fed. Cir. 1996).....                              | 28             |
| <i>Warner-Jenkinson Co. v. Hilton Davis Chemical Co.</i> , 520 U.S. 17 (1997) .....                      | 29             |

**STATUTES**

*35 U.S.C. § 112* .....15, 16